Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Verslag toezicht wettelijke hackbevoegdheid politie 2021

Toezicht op de toepassing door de politie van de bevoegdheid tot het binnendringen en doen van onderzoek in een geautomatiseerd werk.

Inhoudsopgave

Voorwoord 3
1 Inleiding 4
1.1 Aanleiding en doelstelling 4
1.2 Aanpak en afbakening 5
2 Uitgevoerde toezichtactiviteiten 7
3 Resultaten van het onderzoek 8
4 Conclusie 10
Bijlage A: Detailbevindingen 11
A.1 Voorbereiding 11
A.2 Binnendringsoftware en melden onbekende kwetsbaarheden 13
Melden onbekende kwetsbaarheden 14
A.3 Keuring technisch hulpmiddel 14
A.4 Uitvoering binnendringen en verrichten van onderzoekshandelingen 17
Onderzoekshandelingen met een technisch hulpmiddel 20
Onderzoekshandelingen middels handmatige inzet 24
Functiescheiding tussen technisch team en tactisch team 25
A.5 Logging en andere verslaglegging 26
A.6 Bewerking en verstrekking van vastgelegde gegevens 32
A.7 Bewaartermijnen, verwijdering en vernietiging gegevens 33
A.8 Informatiebeveiliging, kwaliteitssysteem en interne controle 34
Kwaliteitssysteem en interne controle 35
Bijlage B: Afkortingen 37

Voorwoord

Dit is het derde verslag waarin de Inspectie Justitie en Veiligheid rapporteert over de inzet van de bevoegdheid door de politie om een geautomatiseerd werk dat in gebruik is bij een verdachte, heimelijk en op afstand binnen te dringen en hier onderzoek in te doen. Deze wettelijke hackbevoegdheid is geïntroduceerd met de inwerkingtreding van de Wet Computercriminaliteit III (Wet CCIII) op 1 maart 2019.

De wetgever hecht grote waarde aan een rechtmatige en zorgvuldige inzet van deze bevoegdheid. Dit is belangrijk om de inbreuk op de privacy van de betrokkenen zoveel mogelijk te beperken en de betrouwbaarheid van de vergaarde gegevens te waarborgen. Door de wetgever zijn regels gesteld om dit doel te bereiken. De Inspectie Justitie en Veiligheid houdt op grond van de Politiewet 2012 toezicht op de naleving van deze regels door de politie. Het belang van het toezicht door de Inspectie wordt mede ingegeven doordat het toezicht zowel de gevallen omvat die de officier van justitie in het kader van strafvervolging aan de rechter voorlegt, als gevallen die niet tot strafvervolging leiden.

In dit verslag rapporteert de Inspectie over de naleving van de regels door de politie bij het toepassen van de hackbevoegdheid in de periode 1 januari 2021 tot en met 31 december 2021.

Hoewel niet op alle vlakken vooruitgang geboekt is, stel ik vast dat de politie in 2021, ten opzichte van de situatie in 2019 en 2020, verbeteringen heeft ingezet en doorgevoerd. Op enkele onderwerpen, waaronder de inzet van commerciële binnendringsoftware en technische hulpmiddelen, signaleer ik spanning tussen de wettelijke kaders en de uitvoeringspraktijk. Het is van belang dat – mede in het licht van de evaluatie van de Wet CCIII – hier aandacht aan wordt besteed. Het WODC doet hier momenteel onderzoek naar.

Als interne borging van de beveiliging van informatie en systemen van de politie en de kwaliteit van de uitvoering door de politie goed zijn ingeregeld, kan het toezicht door de Inspectie Justitie en Veiligheid minder intensief worden uitgevoerd. In de twee eerdere verslagen van de Inspectie gaven we aan dat die twee aspecten niet op orde waren. Ook nu signaleert de Inspectie op deze punten tekortkomingen. Zolang dit nog niet goed is geregeld, ziet de Inspectie het als haar verantwoordelijkheid en rol om het toezicht in 2022 met dezelfde diepgang uit te voeren als over de afgelopen periode. De Inspectie gaat in 2022 tevens onderzoek doen naar de algemene kwaliteitszorg binnen de Politie.

H.C.D. Korvinus
Inspecteur-generaal Inspectie Justitie en Veiligheid

1 Inleiding

1.1 Aanleiding en doelstelling

De Wet computercriminaliteit III (hierna Wet CCIII) verschaft de politie de bevoegdheid om onder strikte voorwaarden een geautomatiseerd werk (een apparaat zoals een laptop of smartphone) dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen. In de media wordt deze bevoegdheid de 'hackbevoegdheid' genoemd.[1] De bevoegdheid mag uitsluitend worden ingezet in geval van verdenking van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert, bij ernstige misdrijven in georganiseerd verband of bij aanwijzingen van een terroristisch misdrijf.[2]

De wetgever hecht grote waarde aan een rechtmatige en zorgvuldige inzet van deze bevoegdheid. Dit is belangrijk om de inbreuk op de privacy van de betrokkenen zoveel mogelijk te beperken en de betrouwbaarheid van de vergaarde gegevens te waarborgen. Door de wetgever zijn regels gesteld om dit doel te bereiken. De wetgever heeft daarbij tevens voorzien in een stelsel van maatregelen van controle en toezicht om de naleving van deze regels te waarborgen. Als onderdeel van dat stelsel is een rol weggelegd voor de Inspectie Justitie en Veiligheid (hierna: de Inspectie). De Inspectie is op grond van de Politiewet 2012 belast met het toezicht op de kwaliteit van de taakuitvoering door de politie. Het toezicht door de Inspectie op de uitvoering van het bevel van de officier van justitie en op de naleving van de wet- en regelgeving rond de toepassing van de hackbevoegdheid is verder verankerd in het Wetboek van Strafvordering en het Besluit onderzoek in een geautomatiseerd werk (hierna: Bogw of Besluit).[3] Hierbij is tevens geregeld dat het toezicht van de Inspectie zich ook richt op de buitengewoon opsporingsambtenaren en bijzondere opsporingsdiensten.[4]

Het toezicht door de Inspectie op de naleving van deze regels en voorschriften heeft mede tot doel om risico's te signaleren en om de politie aan te zetten tot verbetering.

De Inspectie rapporteert inmiddels voor de derde keer over de inzet van de hackbevoegdheid door de politie. In haar verslag over 2020 signaleerde de Inspectie als risico dat verbeteringen waren uitgebleven en dat het zaak is dat de politie uit onze verslagen lessen trekt en zelf tot verbeteringen komt. De Inspectie heeft vorig jaar dan ook aangegeven dat zij haar toezicht in 2021 met dezelfde diepgang en aanpak continueert met een focus op de gesignaleerde tekortkomingen.

[1] Daar waar de term "de bevoegdheid" of "hackbevoegdheid" wordt genoemd, wordt gedoeld op de bevoegdheid om een geautomatiseerd werk dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen.
[2] Zie artt. 126nba, 126uba en 126zpa Wetboek van Strafvordering.
[3] Volledig: Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in artt. 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), Stb. 2018, 340. De wettelijke grondslag van dit besluit is gelegen in artt. 126nba lid 1 en lid 8, 126uba lid 1 en lid 3, 126zpa lid 1 en lid 3, 126ee Wetboek van Strafvordering, en art. 18 lid 1 van de Wet politiegegevens.
[4] Art. 126nba, 7e lid, wetboek van Strafvordering; Staatsblad 2018, nr. 340, p.23, nota van toelichting bij het Besluit onderzoek in een geautomatiseerd werk dat op 9 oktober 2018 in het Staatsblad is gepubliceerd.

1.2 Aanpak en afbakening

Het toezicht door de Inspectie is gericht op het functioneren van het wettelijk systeem rond het toepassen van de hackbevoegdheid door de politie.[5] De uitvoering van de hackbevoegdheid door de politie is centraal belegd bij één technisch team: het Digital Intrusion Team (DIGIT) van de Landelijke Eenheid van de Nationale Politie.[6] Naast politieambtenaren kunnen opsporingsambtenaren van de Koninklijke Marechaussee en opsporingsambtenaren van de bijzondere opsporingsdiensten onderdeel vormen van dit team. Het toezicht door de Inspectie richt zich op de uitvoering door dit team.

Het toezicht omvat zowel de gevallen die de officier van justitie in het kader van strafvervolging aan de rechter voorlegt als gevallen die niet tot strafvervolging leiden.[7]

De Inspectie houdt tevens toezicht op de naleving van de regels en procedures voor de keuring en inzet van software waarmee op apparaten gegevens worden verzameld en de vastlegging van gegevens op een beveiligde technische infrastructuur.[8]

De Inspectie rapporteert in dit verslag over het handelen van de politie in de periode 1 januari 2021 tot en met 31 december 2021.

In 2021 is in de media veel aandacht geweest voor het onderzoek naar SkyECC[9]. Zowel de politie als het Openbaar Ministerie hebben aangegeven dat in dit onderzoek geen sprake is geweest van de inzet van de hackbevoegdheid door Nederlandse opsporingsambtenaren. Dit onderzoek valt daarom buiten de reikwijdte van dit toezicht door de Inspectie.

Medewerkers van DIGIT hebben in 2021 opsporingshandelingen verricht op basis van andere bevoegdheden dan de hackbevoegdheid op grond van de Wet CCIII. Het betreft hier bijvoorbeeld de generieke bevoegdheid tot handhaving van de rechtsorde[10], op grond waarvan de politie bepaalde opsporingshandelingen mag verrichten. Denk hierbij aan het uitvoeren van poortscans[11] en het inloggen op een draadloos netwerk. De politie heeft deze bevoegdheden ingezet in overleg met en in opdracht van het Openbaar Ministerie. Voorts heeft DIGIT in 2021 uitvoering gegeven aan bevelen vanuit het buitenland, op basis van de regelgeving aldaar op geautomatiseerde werken die zich in dat land bevonden. De politie heeft hier eveneens niet gehandeld op basis van de hackbevoegdheid vanuit de Wet CCIII. Deze handelingen vallen daardoor buiten de reikwijdte van het toezicht door de Inspectie op de uitvoering van de hackbevoegdheid.

---

[5] *Kamerstukken II* 2016/17, 34 372, nr.6 p. 106. Het systeemtoezicht wordt uitgeoefend op de uitvoering van de wettelijke regels in de praktijk; Zie Nota van Toelichting bij het Besluit onderzoek in een geautomatiseerd werk dat op 9 oktober 2018 in het Staatsblad is gepubliceerd (Stb. 2018, nr. 340), p 23.

[6] Bogw, nota van toelichting, pagina 14; Bogw, art. 1h definitie technisch team: Onderdeel van de Landelijke Eenheid dat kan worden belast met de uitvoering van een bevel.

[7] Bogw, nota van toelichting, hoofdstuk 5 (toezicht) p. 23; *Kamerstukken II* 2016/17, 34 372, nr.6, p.82.

[8] Bogw, nota van toelichting, paragraaf 3.5 p.20 en artikelsgewijze toelichting hoofdstuk 5 p.37 "*De Inspectie JenV houdt toezicht op de naleving van de technische eisen en de keuringsprocedure*."; Eerste Kamer, 2017-2018, 34 372 G, nadere memorie van antwoord, ontvangen 4 mei 2018, p. 14.

[9] SkyECC was een versleutelde berichtendienst. Zie https://www.om.nl/actueel/nieuws/2021/03/09/nieuwe-klap-voor-georganiseerde-misdaad

[10] Art. 3 Politiewet 2012 juncto art. 141 Wetboek van Strafvordering.

[11] Onder andere om te achterhalen welke applicaties vanaf het internet benaderbaar zijn op een computersysteem.

Rechtskader

De Inspectie heeft zich bij de beoordeling van de toepassing van de hackbevoegdheid gebaseerd op het toepasselijke rechtskader, waarvan de kern wordt gevormd door de Wet CCIII en het Bogw. Voor de nadere duiding van de hierin opgenomen regels en hun bedoeling heeft de Inspectie gebruik gemaakt van toelichtingen en verslagen van parlementaire overleggen. Essentie van het rechtskader is enerzijds te waarborgen dat de door de politie tijdens het onderzoek vergaarde gegevens die kunnen dienen als bewijs in een strafzaak betrouwbaar, integer en herleidbaar zijn. En anderzijds dat de inbreuk op de privacy van de betrokkenen zoveel mogelijk wordt beperkt.

Bij het toezicht op de kwaliteit van de taakuitvoering[12] door de politie betrekt de Inspectie de voor de politie geldende regels, inclusief de randvoorwaarden die nodig zijn om daaraan te kunnen voldoen. Een juiste, tijdige, volledige, aantoonbare en controleerbare uitvoering van de bevoegdheid en het daarover door middel van eigen controles kunnen afleggen van verantwoording zijn belangrijke kwaliteitsaspecten.

Bij het toetsen van open normen uit dit rechtskader heeft de Inspectie 'professional judgement' gehanteerd door toepassing van de kennis en ervaring van de inspecteurs.

Aanwijzingen door het Openbaar Ministerie

De zaaksofficier van justitie heeft de leiding en de eindverantwoordelijkheid over het opsporingsonderzoek waarin de hackbevoegdheid wordt ingezet.[13] De landelijk officier van justitie voor Digital Intrusion (hierna: DIGIT officier van justitie) heeft de leiding over en is verantwoordelijk voor de uitvoering van het bevel door het technisch team.[14] De officier van justitie kan aanwijzingen geven aan de politie.[15] Indien de Inspectie constateert dat de politie afwijkt van de aan haar gestelde regels, gaat de Inspectie na of dit op aanwijzing van de officier van justitie is gebeurd. Het oordelen over het handelen van de officier van justitie valt buiten de toezichtbevoegdheid van de Inspectie.

Relatie met het toezicht van de Procureur-Generaal van de Hoge Raad en de Autoriteit persoonsgegevens

De Inspectie kan in aanraking komen met mogelijke schendingen van de wettelijke voorschriften door, of in opdracht van een officier van justitie. Indien dit zich voordoet, kan de Inspectie de procureur-generaal bij de Hoge Raad (PG-HR) informeren.[16] De Inspectie heeft in 2021 geen melding gedaan van mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie.

Indien de Inspectie constateert dat de politie regels schendt rond de bescherming van persoonsgegevens, kan zij de Autoriteit Persoonsgegevens (AP) informeren.[17] De Inspectie heeft in 2021 geen dergelijke melding gedaan bij de AP.

[12] Art. 65, eerste lid Politiewet 2012.
[13] Artt. 132a en 148 Wetboek van Strafvordering.
[14] Instructie voor de inzet van de bevoegdheid ex. artt. 126nba, 126uba, 126zpa en 126ffa Sv (2021I002)
[15] Art. 12 lid 2 Politiewet 2012.
[16] *Kamerstukken II* 2016-2017, 34 372, nr.6, p. 83.
[17] *Kamerstukken II* 2016-2017, 34 372, nr. 6. p. 83.

2 Uitgevoerde toezichtactiviteiten

De Inspectie heeft toezicht gehouden op alle zaken waarin de bevoegdheid tot het binnendringen en het doen van onderzoek in een geautomatiseerd werk door de politie is toegepast. Onderstaande tabel geeft inzicht in het aantal zaken waarin deze bevoegdheid in 2021 is ingezet.[18] Tevens is hierin opgenomen in hoeveel zaken de politie commerciële binnendringsoftware en door hen aangetroffen onbekende kwetsbaarheden heeft gebruikt. Ten slotte is in de tabel opgenomen hoeveel technische hulpmiddelen de politie heeft laten keuren en hoeveel hiervan zijn goedgekeurd.

Onderwerp	**Aantal**
Totaal aantal zaken waarin DIGIT bevel heeft gekregen om in 2021 de wettelijke hackbevoegdheid toe te passen op grond van de Wet CCIII	28[19]
Aantal van deze zaken waarin bevel is gegeven voor de inzet van een vooraf goedgekeurd technisch hulpmiddel	*2*
Aantal van deze zaken waarin bevel is gegeven voor de inzet van een niet vooraf gekeurd technisch hulpmiddel	*24*
Aantal van deze zaken waarin bevel is gegeven voor het verrichten van onderzoekshandelingen zonder technisch hulpmiddel[20]	*5*
Aantal van deze zaken waarin commerciële binnendringsoftware is ingezet	*23*
Aantal van deze zaken waarin door de politie aangetroffen onbekende kwetsbaarheden door DIGIT zijn gebruikt	*0*
Aantal ter keuring aangeboden technische hulpmiddelen	*7*
Aantal van deze technische hulpmiddelen die zijn goedgekeurd	*5*

De Inspectie is per inzet van de hackbevoegdheid door DIGIT nagegaan of de politie zich gehouden heeft aan de gestelde regels en of zij de verrichte handelingen juist en volledig heeft verantwoord. Hiertoe heeft de Inspectie de aanpak en uitvoering per inzet gereconstrueerd op basis van beschikbare logging, documentatie en interviews. Verder heeft de Inspectie onderzoek verricht naar de uitgevoerde keuringen van technische hulpmiddelen en diverse zaak-overstijgende aspecten, zoals de logging en de beveiliging van de technische infrastructuur van DIGIT.

[18] De Inspectie hanteert als uitgangspunt in de telling dat (een deel van) de periode van een afgegeven bevel voor de toepassing van de hackbevoegdheid in een zaak valt binnen de periode waarover de Inspectie in dit verslag rapporteert, namelijk 1 januari t/m 31 december 2021.

[19] Per zaak kunnen meerdere bevelen voor de inzet van de hackbevoegdheid zijn afgegeven, waaronder eventuele verlengingen, aanvullingen of wijzigingen. In vijf van deze zaken is de eerste inzet reeds gestart in 2020 of eerder.

[20] In één zaak kunnen zowel bevelen afgegeven zijn voor het verrichten van onderzoekshandelingen met als zonder (vooraf goedgekeurd) technisch hulpmiddel.

3 Resultaten van het onderzoek

De toepassing van de hackbevoegdheid door de politie is gereguleerd via wet- en regelgeving. Dit rechtskader beoogt enerzijds te waarborgen dat de tijdens het onderzoek vergaarde gegevens die kunnen dienen als bewijs in een strafzaak betrouwbaar, integer en herleidbaar zijn. En anderzijds dat de inbreuk op de privacy van de betrokkenen zoveel mogelijk wordt beperkt.

De Inspectie is per inzet van de hackbevoegdheid door de politie nagegaan of DIGIT zich gehouden heeft aan de gestelde regels en of zij de verrichte handelingen juist en volledig heeft verantwoord. Hieronder zijn de belangrijkste resultaten van het onderzoek samengevat. In bijlage A zijn de detailbevindingen opgenomen.

Logging en journaal verbeterd

Onder logging verstaat het Besluit de elektronische verslaglegging over de uitvoering van een bevel. Daarnaast kunnen opsporingsambtenaren in een journaal handmatig verslaglegging doen over het procesverloop, de afspraken en de verrichtingen die zich niet lenen voor automatische vastlegging. In 2019 en 2020 rapporteerde de Inspectie dat de logging en het journaal van de door de politie uitgevoerde handelingen onvolledig was. Ook in het begin van 2021 was de logging niet compleet. In de loop van het jaar zijn deze problemen grotendeels verholpen door verbeteringen in de techniek. De logging was accurater en volledi ger. Door diverse soorten logging te combineren met het journaal, heeft de Inspectie de uitgevoerde handelingen in voldoende mate kunnen reconstrueren om een goed beeld te krijgen van de manier waarop de politie de hackbevoegdheid heeft toegepast. Zie hoofdstuk A.5 voor de detailbevindingen.

Commerciële software is 'black box'

Net als in 2020 heeft de politie in het merendeel van de zaken gebruik gemaakt van commerciële software. Voor zowel de politie als de Inspectie is deze software een 'black box'. Het kenmerk van een 'black-box' is dat de resultaten zichtbaar zijn maar voor de gebruiker niet bekend is hoe de software precies werkt. Hoewel in een addendum bij het contract procedurele afspraken zijn gemaakt met de leverancier, is technisch niet afdwingbaar en controleerbaar wat de leverancier van deze software precies op welk moment doet. De leverancier kan daarbij mogelijk ook toegang verkrijgen tot de tijdens een inzet met deze software verkregen gegevens. De Inspectie heeft er begrip voor dat deze software in het belang van de opsporing wordt ingezet, maar signaleert dat hierdoor spanning ontstaat met het rechtskader. In het rechtskader is namelijk aangegeven dat de verkregen gegevens uitsluitend toegankelijk mogen zijn voor de door de korpschef aangewezen ambtenaren. Zie hoofdstuk A.4 voor de detailbevindingen.

Kwaliteitssysteem in opbouw

De Inspectie houdt toezicht op de kwaliteit van de taakuitvoering door de politie. Een intern kwaliteitssysteem waaronder een eigen interne controle is een belangrijk onderdeel voor het borgen van deze kwaliteit. Met een dergelijk systeem kan de politie zelf de kwaliteit van de inzet van de bevoegdheid tijdens alle fasen van de uitvoering borgen en eventuele onregelmatigheden en tekortkomingen hierin tijdig identificeren en verhelpen. In haar verslag over 2020 constateerde de Inspectie dat de politie niet

beschikte over een goed functionerend kwaliteitssysteem inclusief interne controle. In 2021 heeft de politie initiatieven genomen voor het verbeteren en bewaken van de kwaliteit in de uitvoering bij het toepassen van de hackbevoegdheid. De Inspectie stelt vast dat met deze initiatieven in 2021 door de politie zelf tijdig enkele fouten zijn gesignaleerd en ook voorkomen. De politie heeft op onderdelen de kwaliteit verbeterd door eigen controles in te richten. Wat nog ontbreekt, is een overkoepelende analyse waarbij de politie per activiteit van de inzet van de bevoegdheid nagaat welke kwaliteitsborging nodig is om risico's in het gehele proces van uitvoering voldoende te beperken. Tevens ontbreekt documentatie om de kwaliteit van de taakuitvoering te borgen en te voorkomen dat dit uitsluitend rust op de professionele inschatting van individuele medewerkers. Zie hoofdstuk A.8 voor de detailbevindingen.

Informatiebeveiliging niet aantoonbaar op niveau

De beheersing van beveiligingsrisico's is van belang om te waarborgen dat passende beheersingsmaatregelen voor de betrouwbaarheid en integriteit van de logging en de technische infrastructuur getroffen worden en zijn. Dit vormt de basis om door de politie vanuit een interne verantwoordelijkheid toe te zien op het inrichten van deze maatregelen, de structurele naleving daarvan en daarover op een controleerbare wijze verantwoording af te kunnen leggen. De Inspectie ziet hierop toe vanuit haar toezicht op de kwaliteit van de taakuitvoering door de politie. In 2020 was de politie gestart met een traject voor het verbeteren van het aantoonbaar treffen en waarborgen van het beveiligingsniveau van de informatie en informatiesystemen die zij gebruikt bij het toepassen van de hackbevoegdheid. In 2021 is op dit gebied geen vooruitgang geboekt. De Inspectie stelt vast dat de politie hierdoor niet kan aantonen dat haar processen en systemen voldoen aan de eigen gestelde eisen voor informatiebeveiliging. Zie hoofdstuk A.8 voor de detailbevindingen.

Kwetsbare personele bezetting keuringsdienst

Het uitgangspunt is dat onderzoekshandelingen worden verricht met een hiervoor goedgekeurde softwareapplicatie. De beoordeling of deze softwareapplicaties voldoen aan de eisen wordt uitgevoerd door een keuringsdienst. De minister heeft de keuringsdienst van de Landelijke Eenheid van de politie hiervoor aangewezen. De Inspectie stelt vast dat de personele bezetting van de keuringsdienst kwetsbaar is. Door omstandigheden was in heel 2021 slechts één medewerker inzetbaar voor de uitvoering van dit type keuringen. De Inspectie stelt vast dat ondanks deze kwetsbaarheid, de keuringsdienst de keuringen van deze technische hulpmiddelen uitgevoerd heeft volgens de daaraan gestelde eisen. Zie hoofdstuk A.3 voor de detailbevindingen.

4 Conclusie

De Inspectie concludeert dat de politie in 2021 verbeteringen heeft doorgevoerd in de toepassing van de hackbevoegdheid. Hoewel de logging, net als de afgelopen twee jaar, ook in 2021 niet volledig was, is in de loop van dit jaar verbetering zichtbaar geworden. Ook het journaal was dit jaar beter op orde dan de afgelopen twee jaar.

De Inspectie heeft geen aanwijzingen dat de politie in 2021 de hackbevoegdheid heeft ingezet buiten de in de bevelen aangegeven systemen. Voorts stelt de Inspectie vast dat de keuringsdienst van de politie, ondanks de kwetsbare personele bezetting, de keuringsprocedure heeft nageleefd.

Net als in 2020 heeft de politie in 2021 in het merendeel van de zaken commerciële software ingezet waarbij de leverancier toegang heeft, zonder dat dit technisch door de politie kan worden gecontroleerd en beperkt. Tegelijkertijd concludeert de Inspectie dat het gebruik van deze software spanning geeft met het rechtskader.

Evenals in 2020 concludeert de Inspectie dat in 2021 nog geen sprake was van een samenhangend kwaliteitssysteem om de kwaliteit van de inzet van de hackbevoegdheid tijdens alle fasen van de uitvoering te borgen. Tevens is geen vooruitgang geboekt in het aantoonbaar waarborgen van de informatiebeveiliging. Interne borging van deze beveiliging en kwaliteit zijn voorwaarden voor een professionele taakuitvoering door de politie en vermindering van het toezicht door de Inspectie.

De Inspectie concludeert dat de politie ten opzichte van de voorgaande twee jaar beter heeft voldaan aan de eisen, toelichtingen en toezeggingen uit het rechtskader. Waar sprake is van afwijkingen, benoemt de Inspectie deze in dit verslag.

Bijlage A: Detailbevindingen

Deze bijlage beschrijft de bevindingen van het uitgevoerde toezicht door de Inspectie op de toepassing van de hackbevoegdheid door het technisch team van de politie in 2021. Tevens wordt in deze bijlage ingegaan op bevindingen over de keuring van technische hulpmiddelen en op de keuringsdienst die deze keuringen heeft uitgevoerd.

De voornaamste bevindingen zijn op onderwerp bij elkaar gebracht. De volgorde van de paragrafen sluit zoveel mogelijk aan bij het procesverloop van de toepassing van de hackbevoegdheid zoals dat is beschreven in de nota van toelichting bij het Besluit.

A.1 Voorbereiding

De opsporingsambtenaren die de hackbevoegdheid toepassen maken deel uit van een technisch team. Het Besluit stelt regels aan deze opsporingsambtenaren. Een opsporingsambtenaar moet hiervoor namelijk zijn aangewezen door zijn werkgever en lid of deelnemer zijn van een technisch team. [21] Om lid te kunnen worden van een technisch team moet worden voldaan aan de benodigde kwalificaties waaronder deskundigheid- en ervaringsvereisten.[22] Deze vereisten voor leden van een technisch team zijn vastgelegd in de regeling *kwalificaties opsporingsambtenaren*.[23] Voor deelnemers geldt geen kwalificatie-eis, zij kunnen door de korpschef op incidentele basis voor de duur van het bevel in een concrete zaak worden aangewezen indien zij beschikken over specifieke kennis en vaardigheden die daarvoor nodig zijn.[24]

De Inspectie stelt vast dat in 2021:
- de leden van het technisch team voldeden aan de gestelde kwalificatie-eisen. Deze opsporingsambtenaren zijn door hun werkgever aangewezen voor het mogen toepassen van de bevoegdheid. Namens de korpschef zijn zij daarnaast aangewezen als lid van het technisch team;
- in het merendeel van de zaken de deelnemers pas achteraf, in januari 2022, zijn aangewezen. Daarnaast is de aanwijzing als deelnemer voor deze personen niet op incidentele basis. Dezelfde deelnemers zijn namelijk structureel in meerdere zaken aangewezen. Dit is niet in lijn met de toelichting bij het Besluit. Het betreft overigens in alle gevallen opsporingsambtenaren die in dienst zijn bij DIGIT. De politie heeft aangegeven dat de huidige regel omtrent incidentele aanwijzing in deze zaken niet uitvoerbaar is.

[21] Art. 3 tweede lid Bogw.
[22] Art. 3 derde lid Bogw.
[23] Regeling van de minister van Justitie en Veiligheid van 15 februari 2019, kenmerk 2429311, houdende regels betreffende de kwalificaties van opsporingsambtenaren die door de korpschef kunnen worden aangewezen als lid van een technisch team.
[24] Art. 4 tweede lid Bogw (incidentele samenwerking) en artikelsgewijze toelichting op het Besluit, artikel 4 p. 35. "*Hierbij kan worden gedacht aan de situatie dat een opsporingsambtenaar van een bijzondere opsporingsdienst met specifieke kennis op het gebied van digitale fraude wordt toegevoegd aan een technisch team in verband met gewenste technische expertise op dit gebied in een bepaald onderzoek.*" Kamerstuk 34372 nr.27 p.8 heeft het over "*…ter versterking van de technische expertise van een technisch team in een concrete zaak*". Hieruit kan afgeleid worden dat het specifieke kennis betreft, waarover leden van het technisch team niet beschikken.

Haalbaarheidsonderzoek en plan van aanpak

Volgens de toelichting bij het Besluit stelt het technisch team in de voorbereidende fase een rapport haalbaarheidsonderzoek op waarin aandacht wordt besteed aan de haalbaarheid van het onderzoek en de inschatting en beheersing van risico's. Dit betreft risico's t.a.v. inbreuk op de persoonlijke levenssfeer van de verdachte, gevolgen voor het geautomatiseerde werk, kans op nadeel of schade bij derden, maar ook de kans op ontdekking van de inzet van het technisch team door de betrokkene.[25]

De Inspectie stelt vast dat het technisch team rapporten van haalbaarheidsonderzoeken heeft opgesteld voor alle zaken waarin de officier van justitie aan DIGIT bevel heeft gegeven voor toepassing van de bevoegdheid. De Inspectie stelt vast dat in deze haalbaarheidsonderzoeken aandacht besteed wordt aan de risico's en door het technisch team een uitspraak gedaan wordt over de haalbaarheid. De inschatting van de haalbaarheid en van de risico's is niet altijd in het haalbaarheidsonderzoek onderbouwd, maar volgens de Inspectie gelet op de aard van deze onderzoeken, wel aannemelijk.

In de toelichting bij het Besluit is beschreven dat het technisch team na afgifte van een bevel een plan van aanpak opstelt voor het binnendringen in het geautomatiseerde werk.[26] De gekozen aanpak wordt vervolgens door het technisch team getest in een proefopstelling.[27] Met het testen kan onderzocht worden wat het effect is op onderkenning van het onderzoek en hoe de kans daarop beperkt kan worden en van welke eventuele gevolgschade door het binnendringen sprake is. Ook kan getest worden wat het effect van het binnendringen is en in hoeverre daarbij het geautomatiseerde werk na afloop in oorspronkelijke staat achtergelaten kan worden. Een kwaliteitsaspect voor het controleerbaar en betrouwbaar uitvoeren van testen is de aanwezigheid van een testplan, een representatieve testomgeving en van vastlegging van de resultaten van de uitgevoerde test.

De Inspectie stelt vast dat in 2021:

- niet voor elke toepassing van de hackbevoegdheid een plan van aanpak voor het binnendringen aangetroffen is. De status van de wel aanwezige plannen van aanpak is veelal onduidelijk. Deze plannen van aanpak gaan niet altijd in op de wijze en methode van binnendringen waaraan volgens de parlementaire stukken aandacht besteed zou moeten worden;
- een testplan en resultaten van testen in proefopstellingen niet in alle zaken controleerbaar zijn vastgelegd. De Inspectie heeft wel voldoende aanwijzingen dat er getest is. De Inspectie heeft er begrip voor dat de mate waarin het testen plaatsvindt, afhankelijk is van de aard en complexiteit van de zaak en de daartoe in te zetten middelen;
- testen niet altijd zijn uitgevoerd in een testomgeving die controleerbaar representatief is.

De politie heeft in een reactie aangegeven dat gewerkt wordt aan een nieuwe opzet van de haalbaarheidsonderzoeken en plannen van aanpak. Deze nieuwe opzet was nog niet beschikbaar in 2021.

[25] *Kamerstukken II* 2015/16, 34 372 nr.3 p. 33.
[26] Bogw, nota van toelichting, p. 16.
[27] *Kamerstukken I* 2018/2019 34 372, verslag EK 2017/2018, nr. 34, item 5

A.2 Binnendringsoftware en melden onbekende kwetsbaarheden

In 2021 heeft DIGIT in 23 zaken commerciële binnendringsoftware ingezet. Aan de inzet van deze commerciële binnendringsoftware zijn strenge voorwaarden verbonden, waaronder:

- De leverancier is gescreend door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en levert niet aan dubieuze regimes.[28] In parlementaire stukken is niet uitgewerkt op welke aspecten de leverancier door de AIVD wordt gescreend. Deze screening is anders van inhoud dan de veiligheidsonderzoeken die de AIVD uitvoert voor personen die een vertrouwensfunctie (gaan) vervullen. De toets of de leverancier niet levert aan dubieuze regimes wordt uitgevoerd door de politie. Door de minister van JenV is bepaald onder welke condities een regime als dubieus wordt aangemerkt.[29]
- Het functioneren van de binnendringsoftware wordt gecontroleerd in een testomgeving.[30] Dit is onder meer van belang met het oog op het voorkomen van schade aan derden.
- Een product of licentie wordt ingekocht per zaak, waarbij hergebruik na het onderzoek niet mogelijk is, omdat het softwarepakket wordt verwijderd of de licentie is verbruikt.[31]

Zoals de Inspectie in haar verslagen over 2019 en 2020 heeft vermeld, is volgens de daartoe vastgestelde procedure, screening van de betreffende leverancier bij de AIVD aangevraagd en is de toets aangaande het niet leveren aan dubieuze regimes door de politie uitgevoerd door een verklaring hierover op te vragen bij de leverancier. Afgevraagd kan worden, wat de waarde is van een dergelijke eigen verklaring die niet inhoudelijk wordt getoetst. De Inspectie merkt tevens op dat wet- en regelgeving niet verplicht tot het periodiek doorlopen van het proces van de screeningsaanvraag en de toets of de leverancier niet levert aan dubieuze regimes. De screeningsaanvraag en toets hebben dan ook eenmalig al in 2019 plaatsgevonden.

Voorafgaand aan de inzet is de binnendringsoftware in deze zaken beperkt getest in een testopstelling. Zie hierover hoofdstuk A.1 (voorbereiding) en hoofdstuk A.4 (uitvoering).

De Inspectie heeft vastgesteld dat per zaak waarin commerciële binnendringsoftware succesvol is ingezet, één licentie is ingekocht nadat is binnengedrongen. De Inspectie heeft er begrip voor dat licenties pas na succesvol binnendringen worden aangeschaft om onnodige kosten te vermijden. Hergebruik is mogelijk omdat na afronding van eerdere onderzoeken het softwarepakket niet wordt verwijderd en de licentie niet is verbruikt.

Commerciële binnendringsoftware maakt soms gebruik van fouten in software die nog onbekend zijn bij de producent van deze software. Uit de parlementaire behandeling blijkt dat de eis tot de aanschaf van licenties in een zaak is bedoeld voor het zo min mogelijk stimuleren van de markt voor dit soort kwetsbaarheden en de daaraan

[28] *Kamerstukken II* 2017/18, 34 372 nr. 27 p.7; Regeerakkoord 2017-2021 "Vertrouwen in de toekomst" p.3.
[29] *Kamerstukken II* 2018/19, 35 257 nr. 3 p. 20; Beantwoording op 24 juli 2019 van Kamervragen over een media bericht over WhatsApp. Kenmerk 2647151.
[30] Bogw, nota van toelichting, hoofdstuk 3.3, p.16, hoofdstuk 3.5, p.18 en p.20.
[31] Bogw, nota van toelichting, hoofdstuk 3.3 p.15 en p.16.

verbonden negatieve gevolgen voor de veiligheid van het internet.[32] De Inspectie signaleert, evenals over de twee afgelopen jaren, dat in de praktijk het voorgeschreven licentiemodel juist leidt tot extra kosten voor de politie en daarmee mogelijk tot een extra stimulans voor deze markt.

Melden onbekende kwetsbaarheden

Softwarecode bevat in zijn algemeenheid vrijwel altijd fouten. Onbekende kwetsbaarheden zijn fouten in software die nog onbekend zijn bij de producent van deze software. Er zijn partijen die bereid zijn veel geld te betalen voor informatie over bepaalde onbekende kwetsbaarheden. Om deze markt voor onbekende kwetsbaarheden niet te stimuleren, is het uitgangspunt dat als de politie beschikt over informatie van onbekende kwetsbaarheden[33] hiervan melding gemaakt wordt aan de producent.[34] De meldingsplicht is overigens niet wettelijk verankerd: in het Wetboek van Strafvordering is alleen het uitstel van een melding van een onbekende kwetsbaarheid geregeld. Wel is de meldplicht benoemd in een Kamerbrief.[35] In een ander Kamerstuk is aangegeven dat de officier van justitie dit uitstel uitsluitend kan bevelen op grond van een zwaarwegend opsporingsbelang en na machtiging van een rechter-commissaris.[36] Dit impliceert dat de officier van justitie bij de afweging voor uitstel tevens beoordeelt of sprake is van een onbekende kwetsbaarheid zoals bedoeld in artikel 126ffa van het Wetboek van Strafvordering.

In 2021 heeft DIGIT in twee opsporingsonderzoeken kwetsbaarheden aangetroffen die kunnen worden gebruikt om een geautomatiseerd werk binnen te dringen. De Inspectie heeft vastgesteld dat DIGIT deze kwetsbaarheden ter beoordeling, conform de werkproces afspraken, voorgelegd heeft aan de DIGIT officier van justitie. In een van deze gevallen heeft de DIGIT officier van justitie besloten dat het daadwerkelijk een of meerdere onbekende kwetsbaarheden betreft. In dit geval heeft de officier van justitie bevolen dat het bekend maken hiervan aan de producent wordt uitgesteld. Overigens heeft DIGIT deze kwetsbaarheden in 2021 niet daadwerkelijk gebruikt om een geautomatiseerd werk binnen te dringen.

A.3 Keuring technisch hulpmiddel

Na het binnendringen voert het technisch team onderzoek uit in het apparaat. In het Wetboek van Strafvordering is aangegeven dat bij het verrichten van onderzoekshandelingen al dan niet gebruik kan worden gemaakt van een technisch hulpmiddel.[37] Volgens het Bogw is een *technisch hulpmiddel* 'een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel'.[38] Om de betrouwbaarheid en integriteit van technische hulpmiddelen, de betrouwbaarheid en integriteit van de hiermee

[32] Zie *Kamerstukken I 2016/17, 34 372, E,* p. 4 en p. 11 en *Kamerstukken I 2016/17, 34 372, D (MvA I),* p. 20-22.
[33] Onder onbekende kwetsbaarheid wordt volgens Sv. artikel 126ffa vierde lid verstaan "een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen."
[34] Kamerstukken II 2016/17, 34 372 nr.6, p.9.
[35] Kamerstukken I 2016/17, 26 643, nr. 428, pagina 4.
[36] Bogw, nota van toelichting, p.31; Sv. Artikel 126ffa derde lid.
[37] Artt. 126nba, 126uba, 126zpa eerste lid, Wetboek van Strafvordering.
[38] Staatsblad 2018, nr. 340, art. 1g. Besluit onderzoek in een geautomatiseerd werk,

geregistreerde gegevens en de herleidbaarheid van de gegevens te borgen, stelt het Besluit diverse technische eisen[39] aan een technisch hulpmiddel.[40]

Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er volgens de toelichting bij het Besluit vanuit worden gegaan dat aan de wettelijke eisen met betrekking tot betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan.[41] Daarnaast biedt een goedgekeurd technisch hulpmiddel als voordeel dat risico's op misbruik door derden worden beperkt en dat specificaties van het middel niet worden prijsgegeven. Dit is van groot belang voor de afscherming van gevoelige opsporingsmethoden.[42]

De beoordeling of een technisch hulpmiddel voldoet aan de eisen wordt uitgevoerd door een keuringsdienst. De minister heeft de keuringsdienst van de Landelijke Eenheid aangewezen als keuringsdienst voor de keuring van technische hulpmiddelen.[43]

In 2020 werden deze keuringen nog uitgevoerd door de aangewezen keuringsdienst TNO. Sinds 2021 keurt de keuringsdienst van de Landelijke Eenheid van de politie in het kader van de hackbevoegdheid zelfstandig deze technische hulpmiddelen.

De Inspectie constateert dat de personele bezetting van de keuringsdienst van de Landelijke Eenheid kwetsbaar is. Door omstandigheden was in heel 2021 slechts één medewerker inzetbaar voor de uitvoering van dit type keuringen. Deze medewerker is in 2021 op afroepbasis ondersteund en gecontroleerd door medewerkers van TNO. Met deze tijdelijke ondersteuning door TNO kon de keuringsdienst van de Landelijke Eenheid in 2021 invulling geven aan de eigen gestelde minimale kwaliteitsvereisten van een vier-ogen principe. Begin 2021 was door de keuringsdienst voorzien dat haar personele capaciteit voor deze taak zou worden uitgebreid. De Inspectie constateert dat in heel 2021 geen sprake is geweest van deze uitbreiding.

Aan de keuringsdienst van de Landelijke Eenheid zijn geen specifieke eisen gesteld, zoals deze wel voor de aangewezen keuringsdienst TNO in 2020 golden.[44] Dergelijke eisen bieden waarborgen om de kwaliteit, capaciteit en beschikbaarheid van middelen zeker te stellen. De Inspectie merkt op dat het Besluit de ruimte biedt om middels een ministeriele regeling eisen te stellen aan de keuringsdienst van de Landelijke Eenheid.

In het Besluit is gespecificeerd aan welke eisen een technisch hulpmiddel moet voldoen om te worden goedgekeurd. De wijze van keuring en keuringscriteria zijn door de keuringsdienst op hoofdlijnen vastgelegd in een keuringsprotocol dat door de minister is goedgekeurd.[45] De Inspectie stelt vast dat de minister van Justitie en Veiligheid op 28 februari 2021 het door de keuringsdienst van de Landelijke Eenheid opgestelde keuringsprotocol heeft goedgekeurd. De keuring van technische hulpmiddelen moet

[39] Artt. 8 t/m 13 Bogw.
[40] Bogw, nota van toelichting hoofdstuk 3.5 pagina 18.
[41] Bogw Nota van Toelichting 3.5 pagina 19.
[42] *Kamerstukken II* 2015/16, 34 372, nr. 3 memorie van toelichting Wet CCIII, p.110.
[43] Art. 16 eerste lid Bogw (aanwijzing onderdeel Landelijke Eenheid als keuringsdienst).
[44] Staatscourant nr.10713, 27 februari 2019. Regeling eisen keuringsdienst technisch hulpmiddel, 15 februari 2019, nr. 2433978.
[45] Art. 17 Bogw (keuringsprotocol) en artikelsgewijze toelichting artikelen 16 t/m 19, p.42.

worden uitgevoerd op basis van dit keuringsprotocol.[46] Dit nieuwe keuringsprotocol is inhoudelijk vrijwel identiek aan het keuringsprotocol van TNO.

In 2021 is namens de korpschef zeven keer een technisch hulpmiddel ter keuring aangeboden. Bij vijf uitgevoerde keuringen is de keuringsdienst van oordeel dat het aangeboden technisch hulpmiddel voldoet aan de gestelde eisen uit het Besluit. De Inspectie heeft vastgesteld dat door de keuringsdienst voor elk goedgekeurd technisch hulpmiddel testactiviteiten zijn uitgewerkt die aansluiten op het keuringsprotocol.

De Inspectie is per keuringseis nagegaan hoe en op basis waarvan de keuringsdienst tot haar oordeel is gekomen. De Inspectie stelt vast dat:
- de keuringsuitslagen op een systematische en navolgbare wijze tot stand gekomen zijn;
- het onderliggende keuringsdossier gestructureerd en goed toegankelijk is;
- verantwoording over de uitgevoerde testactiviteiten, bijbehorende uitkomsten en afwegingen gestructureerd en op een controleerbare wijze zijn vastgelegd in een voor dit doel ontwikkelde voorziening. Hieruit is voor de Inspectie in voldoende mate af te leiden in hoeverre het betreffende technische hulpmiddel voldoet aan de hieraan gestelde technische eisen[47] en is navolgbaar hoe en op basis waarvan de keuringsdienst tot goedkeuring is gekomen;
- het keuringsrapport van de goedgekeurde technische hulpmiddelen voldoet aan de daaraan gestelde eisen.[48]Tevens heeft de keuringsdienst bij elk goedgekeurd technisch hulpmiddel een handleiding opgesteld;[49]
- door de keuringsdienst een centrale registratie bijgehouden wordt van de keuringsrapporten;[50]

De Inspectie heeft waargenomen dat de keuringsdienst naar aanleiding van de inspectiebezoeken gedurende het jaar direct aan de slag is gegaan om verbeteringen in haar werkprocessen door te voeren.

Op basis van het keuringsdossier was voor de Inspectie niet altijd precies duidelijk hoe ver de afbakening van de keuring reikte (wat is wel en niet meegenomen). Door de Inspectie wordt het niet expliciet maken van beperkingen en uitsluitingen in de keuringsdossiers als gemis ervaren. Hierdoor kunnen mogelijk andere verwachtingen en beelden ontstaan ten aanzien van een goedgekeurd product.

De Inspectie wijst voorts op mogelijkheden om in voorkomende gevallen aan de hand van broncode de keuring voor specifieke testonderdelen efficiënter en effectiever uit te voeren en daarmee meer zekerheid te kunnen bieden.

Het Besluit biedt de keuringsdienst de ruimte om vervangende waarborgen te stellen op onderdelen waar het technisch hulpmiddel niet voldoet aan in het Besluit gestelde technische eisen.[51] Deze verplicht te treffen vervangende waarborgen worden door de

[46] Bogw, artikelsgewijze toelichting artikel 17, p.42.
[47] Hoofdstuk 5 Bogw.
[48] Art. 18 Bogw.
[49] Bogw, artikelsgewijze toelichting artikel 9, p.38.
[50] Art. 19 Bogw
[51] Bogw, artikelsgewijze toelichting artikel 18, p.43 vermeldt verplicht te treffen vervangende procedurele waarborgen. Dit kan tot verwarring leiden. Voor de uniformiteit hanteert de Inspectie hier het begrip "vervangende waarborgen".

keuringsdienst in het keuringsrapport vastgelegd.[52] In alle keuringsrapporten van de goedgekeurde technische hulpmiddelen zijn door de keuringsdienst verplicht te treffen vervangende waarborgen benoemd. Deze zijn volgens de Inspectie duidelijk genoeg geformuleerd, maar niet altijd uitvoerbaar in de praktijk. Het risico is dat in die situaties het ingezette technisch hulpmiddel niet voldoet aan de gestelde voorwaarden voor goedkeuring.

Samenvattend concludeert de Inspectie dat de keuringsdienst van de Landelijke Eenheid de keuringen heeft uitgevoerd volgens de daaraan gestelde eisen en dat het gevolgde keuringsproces en de totstandkoming van de keuringsuitslag navolgbaar is. Een zorgpunt is de kwetsbare personele bezetting van de keuringsdienst waardoor er risico's gelopen worden in de continuïteit en kwaliteit van deze keuringen.

A.4 Uitvoering binnendringen en verrichten van onderzoekshandelingen

Het op afstand en heimelijk binnendringen en het verrichten van onderzoek in een geautomatiseerd werk kan worden uitgevoerd zodra daartoe, na machtiging van de rechter-commissaris, een bevel is afgegeven door de officier van justitie.

In het bevel specificeert de officier van justitie de onderzoeksdoelen waarvoor de bevoegdheid in een bepaalde zaak door de politie ingezet mag worden. De opsporingsambtenaar van het technisch team mag alleen handelingen uitvoeren die passen binnen deze afgegeven doelen. De mogelijke onderzoeksdoelen zijn limitatief in het Wetboek van Strafvordering omschreven.[53] Het betreft de doelen:

- de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker zoals de identiteit of locatie, en de vastlegging daarvan;
- het opnemen van vertrouwelijke communicatie (ovc) of het aftappen en opnemen van telecommunicatie;[54]
- stelselmatige observatie, waarbij door de officier van justitie bepaald kan worden dat het technisch hulpmiddel op de persoon wordt bevestigd;[55]
- de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen (historische gegevens) of die binnen de looptijd van het bevel nog worden opgeslagen;
- de ontoegankelijk making van gegevens.

De totstandkoming van de afgifte en de inhoud van een bevel is de verantwoordelijkheid van de officier van justitie en valt daarmee buiten de reikwijdte van het toezicht door de Inspectie. Het door de officier van justitie afgegeven bevel vormt wel het kader waarbinnen de politie uitvoering aan de hackbevoegdheid moet geven. In het bevel vermeldt de officier van justitie naast de eerdergenoemde doelen, het nummer of een andere aanduiding van het geautomatiseerde werk en ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering

[52] Art. 18, derde lid, sub e. "*Het keuringsrapport van een goedgekeurd technisch hulpmiddel vermeldt ten minste: e) relevante verplichte vervangende waarborgen waarmee voldaan kan worden aan één of meer eisen, bedoeld in artikelen 8 tot en met 13*".

[53] Artt. 126nba, 126uba en 126zpa eerste lid Sv.

[54] Aan de uitvoering hiervan ligt respectievelijk een bevel ten grondslag op basis van artikel 126l, Sv. (opnemen van vertrouwelijk communicatie) en artikel 126m, Sv. (opnemen van niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst).

[55] Aan de uitvoering ligt een bevel op basis van 126g, Sv. (stelselmatige observatie) ten grondslag.

gegeven moet worden. Ook vermeldt het bevel het tijdstip of de periode waarbinnen aan het bevel door de politie uitvoering moet worden gegeven.[56] Indien bevel is gegeven voor het opnemen van vertrouwelijke communicatie (ovc)[57], zijn in het bevel de locaties gespecificeerd waar dit mag plaatsvinden.

Deze in het bevel benoemde onderdelen zijn door de Inspectie als kader gehanteerd om te bepalen of het technisch team heeft gehandeld binnen de reikwijdte van het bevel.[58]

De Inspectie stelt vast dat bijna alle in 2021 door DIGIT uitgevoerde opsporingshandelingen vallen binnen de reikwijdte van de hiervoor afgegeven bevelen. Hierbij heeft de Inspectie gekeken naar de in de bevelen aangegeven perioden, doelen en kenmerken van de geautomatiseerde werken. In enkele situaties is daarvan op de volgende onderdelen (mogelijk) afgeweken:

- in één zaak is een technisch hulpmiddel ingezet dat mogelijk standaard locatiegegevens vastlegt bij bepaalde handelingen door de gebruiker van het onderzochte geautomatiseerd werk. De Inspectie signaleert dat deze vastlegging van locatiegegevens mogelijk kenmerken heeft van stelselmatige observatie. In de zaak waarin dit hulpmiddel is ingezet, is echter geen bevel afgegeven voor het middels de hackbevoegdheid stelselmatig observeren van de betreffende verdachte;
- in één zaak is eenmalig als test een geluidsopname gestart op het geautomatiseerde werk van een verdachte, zonder dat daarvoor op dat moment een bevel aan ten grondslag lag. Dat bevel is overigens naderhand op dezelfde dag wel verstrekt;
- in één zaak heeft DIGIT een beëindigingsbevel ontvangen waarmee de looptijd van een eerder gegeven bevel werd verkort. DIGIT was hiervan niet op de hoogte gesteld en ontving dit bevel pas toen het aangegeven beëindigingsmoment reeds was verstreken. In de tussentijd hebben wel onderzoekshandelingen plaatsgevonden. DIGIT heeft hier proces-verbaal voor opgesteld en de betreffende gegevens weggelaten uit de finale overdracht van verzamelde gegevens aan het tactisch team. In een tussentijdse overdracht waren deze gegevens echter reeds overgedragen.

Op de genoemde (mogelijke) afwijkingen na, heeft de Inspectie geen aanwijzingen dat de politie in 2021 de hackbevoegdheid heeft ingezet buiten de in de bevelen aangegeven systemen, periodes en onderzoeksdoelen.

Uitvoering door opsporingsambtenaren
Het binnendringen, het plaatsen en verwijderen van een technisch hulpmiddel en het verrichten van onderzoekshandelingen, al dan niet met een technisch hulpmiddel is voorbehouden aan de opsporingsambtenaren die lid of deelnemer zijn van een technisch team.[59]

In 2021 zijn in 15 zaken onderzoekshandelingen verricht door medewerkers van DIGIT die niet vooraf formeel aangewezen zijn als lid of deelnemer van het technisch team. De aanwijzing als deelnemer van het technisch team in deze zaken heeft namelijk pas

[56] Artt. 126nba,126uba en 126zpa tweede en derde lid Sv.
[57] Hier wordt gedoeld op de afgegeven combibevelen voor de inzet van de bevoegdheid op basis van 126nba (doel b) en 126l Sv. of 126uba (doel b) en 126s Sv.
[58] Artt. 126nba, 126uba en 126zpa zevende lid Sv. "*Het toezicht op de uitvoering van het bevel door de ambtenaren wordt uitgeoefend door de Inspectie overeenkomstig het bepaalde in hoofdstuk 6 van de Politiewet 2012*."
[59] Bogw, nota van toelichting, hoofdstuk 3.3 p.16; Artt. 23 eerste lid, 24 eerste lid en 25 tweede lid Bogw.

achteraf, in januari 2022, plaatsgevonden. Zie tevens hoofdstuk A.1 (voorbereiding). In het vervolg wordt door de Inspectie gesproken over deze deelnemers alsof zij formeel aangewezen zijn. Voor bijna alle zaken in 2021 geldt dat de Inspectie op basis van logging vastgesteld heeft dat de personen die in 2021 opsporingshandelingen hebben verricht of wel lid zijn of wel middels de aanwijzing achteraf als deelnemer aangewezen zijn. In één zaak is door de Inspectie een afwijking geconstateerd. In deze zaak zijn volgens de logbestanden twee keer onderzoekshandelingen verricht door een medewerker van DIGIT die in de betreffende zaak (ook achteraf) niet als deelnemer is aangewezen.

Om de kwaliteit en professionaliteit van het onderzoek te borgen moeten de opsporingsambtenaren die op een ad hoc basis deelnemen aan een technisch team volgens het Besluit gedurende de uitvoering van het onderzoek begeleid worden door een lid van een technisch team.[60]

Aan de begeleiding van deelnemers wordt volgens de politie invulling gegeven door het instrueren van de deelnemers tijdens de briefings. Tevens wordt volgens de politie het zogenaamde vier-ogen principe toegepast. Dit vier-ogen principe betekent dat bij deze zaken ten minste twee personen betrokken zijn bij het binnendringen en het verrichten van onderzoekshandelingen. Tijdens de uitvoering van het bevel behoeven de deelnemers volgens de politie dan ook niet permanent begeleid te worden. De politie geeft aan dat deze invullingswijze in overeenstemming is met de afspraak die daarover met de DIGIT officier van justitie is gemaakt.

De Inspectie leidt uit het journaal af dat in de zaken waar deze deelnemers ingezet zijn, voorzien is in het vier-ogen principe. De Inspectie merkt op dat uit het journaal blijkt dat het vier-ogen principe ook door twee deelnemers ingevuld wordt. De Inspectie heeft begrip voor deze werkwijze gelet op de aard van het technisch hulpmiddel waarvoor deze deelnemers zijn ingezet en de vaststelling dat in 2021 een vaste groep deelnemers in de zaken structureel ingezet is en daarmee ook de nodige kennis en ervaring met het gebruik van het betreffende technisch hulpmiddel opgedaan hebben.

Tijdens de behandeling van het wetsvoorstel CCIII is door de minister aangegeven dat alleen de technische, daartoe aangewezen ambtenaren toegang mogen hebben tot het systeem van waaruit het op afstand binnendringen van het geautomatiseerde werk wordt uitgevoerd.[61] Tevens is door de minister aangegeven dat de geïnfecteerde geautomatiseerde werken niet in verbinding mogen staan met een server van de leverancier van de binnendringsoftware.[62]

In 23 zaken heeft de politie commerciële binnendringsoftware ingezet voor het binnendringen. Net als in 2020 stelt de Inspectie vast dat deze software gebruik maakt van servers die beheerd worden door een leverancier. Naast de daartoe aangewezen ambtenaren heeft dus ook de leverancier toegang tot het systeem waaruit het op afstand binnendringen van het geautomatiseerde werk wordt uitgevoerd.

In de zaken waar op andere wijze is binnengedrongen, heeft de Inspectie vastgesteld dat de systemen van waaruit op afstand is binnengedrongen, in beheer en onder

[60] Art. 4 derde lid Bogw (incidentele samenwerking); Bogw, nota van toelichting, p.36.
[61] *Kamerstukken II* 2016/17, 34 372, nr. 6 p.52.
[62] *Kamerstukken II* 2016/17, 34 372, nr. 6 p.78.

controle staan van de politie. De Inspectie heeft geen aanwijzingen dat ongeautoriseerde toegang heeft plaatsgevonden.

De door de politie ingekochte binnendringsoftware is een 'black box'[63] voor de politie, waarbij door hen niet kan worden uitgesloten dat de geïnfecteerde geautomatiseerde werken in verbinding staan met een server van de leverancier van de binnendringsoftware.

Onderzoekshandelingen met een technisch hulpmiddel

Na het binnendringen voert het technisch team onderzoek uit in het apparaat. Bij het verrichten van onderzoekshandelingen wordt al dan niet gebruik gemaakt van een technisch hulpmiddel.[64] Als voor het verrichten van onderzoekshandelingen een technisch hulpmiddel ingezet wordt, is het uitgangspunt dat dit een vooraf goedgekeurd hulpmiddel betreft.

In 2021 is in 24 zaken een bevel gegeven voor het gebruik van een technisch hulpmiddel voor het uitvoeren van onderzoekshandelingen. Bij twee van deze zaken betreft het een vooraf door de keuringsdienst goedgekeurd technisch hulpmiddel. In de andere 22 zaken heeft de officier van justitie bepaald dat het onderzoeksbelang dringend vordert dat een niet gekeurd technisch hulpmiddel wordt gebruikt.[65] De Inspectie stelt vast dat hiermee niet is tegemoetgekomen aan het uitgangspunt dat een vooraf goedgekeurd hulpmiddel wordt ingezet.

In de situatie dat de officier van justitie bepaald heeft dat het onderzoeksbelang dringend vordert dat een niet gekeurd technisch hulpmiddel wordt gebruikt, beschrijft het Besluit twee mogelijke vervolgtrajecten. In de eerste situatie, wat tevens het uitgangspunt is, vindt keuring achteraf plaats en vermeldt de officier van justitie de uitkomst van de keuring na afloop van het gebruik in de processtukken.[66] In deze situatie bestaat het risico dat het technisch hulpmiddel in combinatie met de getroffen vervangende waarborgen wordt afgekeurd omdat uit de keuring blijkt dat alle mogelijke vervangende waarborgen die achteraf getroffen kunnen worden, naar oordeel van de keuringsdienst onvoldoende blijken te zijn. Terwijl mogelijk wel sprake zou zijn van een goedgekeurd technisch hulpmiddel als bepaalde vervangende waarborgen of instellingen tijdens de inzet waren getroffen.

De Inspectie stelt vast dat in 2021 in één zaak een technisch hulpmiddel achteraf gekeurd is. In deze zaak zijn binnen de looptijd van dat bevel overigens geen onderzoekshandelingen verricht.

Gebruik technisch hulpmiddel waarvan keuring achterwege blijft

In de tweede situatie kan, als uitzondering op de hoofdregel, de keuring van een technisch hulpmiddel geheel achterwege blijven.[67] De officier van justitie is in die situatie van oordeel dat de aard van het technisch hulpmiddel zich verzet tegen

[63] Bij een 'black box' is het gedrag en de exacte werking van een product onbekend bij de afnemer of gebruiker.
[64] Artt. 126nba, 126uba, 126zpa eerste lid, Wetboek van Strafvordering.
[65] Art. 21 tweede lid Bogw.
[66] Art. 15 eerste lid, art. 21 derde lid en artikelsgewijze toelichting bij artikel 21, p. 44, Bogw; *Kamerstukken I* 2017/18, 34 372, nr. G, p.15.
[67] In de artikelsgewijze toelichting artikel 21, p.45 is aangegeven dat de hiervan in de praktijk geen lichtzinnig gebruik van gemaakt zal worden en dat het naar verwachting om uitzonderlijke gevallen gaat.

keuring.[68] In dat geval vermeldt de officier in de processtukken welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen.[69] De aanvullende waarborgen kunnen op aangeven van de officier van justitie ook (deels) buiten de inzet van het technisch team getroffen zijn.

In 2021 is in 23 zaken door de officier van justitie bepaald dat het onderzoeksbelang dringend vordert dat een niet vooraf gekeurd technisch hulpmiddel wordt ingezet. De officier van justitie heeft beslist dat het betreffende middel zich naar zijn aard verzet tegen keuring. In de aanwezige processen-verbaal heeft DIGIT een beschrijving opgenomen van diverse maatregelen die ze op aangeven van de DIGIT officier van justitie heeft getroffen om risico's te mitigeren voor de betrouwbaarheid van de verzamelde gegevens. De Inspectie stelt vast dat het merendeel van deze maatregelen standaard getroffen moeten worden volgens het Besluit en derhalve geen aanvullende waarborgen zijn. Tevens stelt de Inspectie vast dat de politie niet voor elk van de verantwoorde maatregelen kan aantonen dat deze daadwerkelijk zijn getroffen. Eén van deze maatregelen is dat dat het technisch hulpmiddel is getest in een test- en verificatieopstelling.[70] De Inspectie stelt op basis van logging en het journaal vast dat deze testen zijn uitgevoerd. De Inspectie stelt vast dat dit testen op een basale en beperkte wijze plaatsvindt. In enkele gevallen is na afstemming met de DIGIT officier van justitie geen nieuwe test uitgevoerd omdat in andere zaken ervaring opgedaan was met een gelijkend geautomatiseerd werk. De Inspectie stelt vast dat in de gevallen waarin deze testen zijn uitgevoerd, het geautomatiseerde werk waarop is getest zoveel mogelijk gelijkend is aan het geautomatiseerde werk waarop het technisch hulpmiddel daadwerkelijk is ingezet. De Inspectie heeft begrip dat het verkrijgen van identieke omstandigheden bij het testen van dit technisch hulpmiddel een utopie is. Er is daarbij namelijk enerzijds een afhankelijkheid met de daadwerkelijke inrichting van het geautomatiseerde werk in gebruik door de verdachte, waarover niet altijd op voorhand uitsluitsel gegeven kan worden. Anderzijds stelt de Inspectie vast dat het technisch hulpmiddel dusdanig frequent wordt bijgewerkt, dat in de meeste gevallen de versie van het technisch hulpmiddel tijdens de inzet niet identiek is aan de gehanteerde versie in de betreffende test- en verificatieopstelling. Deze constatering leidt ertoe dat de test- en verificatieopstelling als aanvullende waarborg beperkt bijdraagt om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.

Gelet op de aard van de waarborgen die door het technisch team getroffen zijn, merkt de Inspectie op dat uitsluitend het treffen van deze waarborgen onvoldoende lijkt om de betrouwbaarheid van de gegevens te waarborgen. Naast de aanvullende waarborgen van het technisch team, kunnen per zaak op aangeven van de zaaksofficier ook diverse aanvullende waarborgen getroffen zijn door de tactische teams. De door de tactische teams getroffen waarborgen zijn niet door de Inspectie onderzocht. Het oordeel over of en in welke mate het samenstel van waarborgen afdoende is, is in het Nederlandse strafproces uiteindelijk voorbehouden aan de rechter.

[68] Art. 15, tweede lid; artikel 21, vierde lid en artikelsgewijze toelichting artikel 21 p. 45, Bogw.
[69] Art. 21, vierde lid Bogw.
[70] Deze test- en verificatie is gericht op het testen van de functionaliteit van het technisch hulpmiddel voor het verrichten van onderzoekshandelingen. Het testen van het plan van aanpak in paragraaf 2.2 (voorbereiding) is gericht op het binnendringen. Beide kunnen in voorkomende gevallen gecombineerd zijn.

Inzet goedgekeurd technisch hulpmiddel

Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er volgens de toelichting bij het Besluit vanuit worden gegaan dat aan de wettelijke eisen met betrekking tot betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan.[71]

In 2021 is in twee zaken een door de keuringsdienst vooraf goedgekeurd technisch hulpmiddel ingezet. De Inspectie kan echter op basis van logging niet vaststellen dat deze door DIGIT ingezette technische hulpmiddelen identiek zijn aan de middelen die door de keuringsdienst zijn gekeurd.

Het Besluit biedt de keuringsdienst de ruimte om vervangende waarborgen te stellen op onderdelen waar het technisch hulpmiddel niet voldoet aan in het Besluit gestelde technische eisen.[72] Deze door de politie dan verplicht te treffen vervangende waarborgen worden door de keuringsdienst in het keuringsrapport vastgelegd. Het is bij de uitvoering van het bevel dan ook zaak dat DIGIT deze vervangende waarborgen aantoonbaar heeft geïmplementeerd en verantwoording over de naleving aflegt.

In de keuringsrapporten van beide technische hulpmiddelen zijn door de keuringsdienst vervangende waarborgen benoemd. Onderdeel van deze verplicht te treffen vervangende waarborgen is dat DIGIT verantwoording aflegt over het treffen van deze waarborgen in een proces-verbaal. Deze processen-verbaal waren voor de zaken waar deze technische hulpmiddelen zijn ingezet nog niet opgesteld omdat de inzet in 2021 nog niet was afgerond.

Inzet technisch hulpmiddel dat wordt afgekeurd

Indien de situatie zich voor zou doen dat een reeds ingezet hulpmiddel toch achteraf wordt afgekeurd, dan wordt dit voorgelegd aan de rechter in de strafzaak, die beslist over het gebruik van de gegevens als bewijs.[73] In 2021 zijn door DIGIT geen technische hulpmiddelen ingezet die zijn afgekeurd.

Definitie technisch hulpmiddel

De Inspectie constateert dat in 2021 in één zaak programmatuur is ingezet waarvan door de politie en de DIGIT officier van justitie bepaald is dat dit niet over alle kenmerken van een technisch hulpmiddel beschikt. Het automatisch transport naar een technische infrastructuur om de verkregen gegevens vast te leggen ontbreekt hierin namelijk. De politie beschouwt het gebruik van deze programmatuur derhalve als een handmatige inzet, zoals bedoeld in artikel 21 lid 5 Bogw. De Inspectie signaleert echter dat bij een ander middel waar ook geen automatisch transport ingericht is, bepaald is dat dat middel zich naar zijn aard verzet tegen keuring. Dit impliceert dat in die situatie wel sprake is van een technisch hulpmiddel. Deze opstelling is niet consistent.

[71] Bogw Nota van Toelichting paragraaf 3.5 pagina 19.
[72] Art. 18 derde lid sub e Bogw; artt. 16 t/m 18, Bogw, artikelsgewijze toelichting, p.43.
[73] *Kamerstukken II* 2018/19, 34 372, nr. 29, p.13.

Verwijdering van een technisch hulpmiddel

Volgens het Bogw verwijdert een opsporingsambtenaar van het technisch team het technisch hulpmiddel voordat het onderzoek is beëindigd.[74] Hierbij zal worden geprobeerd het geautomatiseerde werk in de oorspronkelijke staat achter te laten, dat wil zeggen als ware de bevoegdheid nooit toegepast.[75]

In 2021 is in 23 zaken bevel gegeven voor de inzet van een technisch hulpmiddel waarvan uitsluitend de leverancier inzicht heeft in de precieze werking van het betreffende middel. Hierdoor kan niet worden vastgesteld of in alle gevallen verwijdering daadwerkelijk volledig heeft plaatsgevonden.

Er kan zich een situatie voordoen dat een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk. In de parlementaire stukken is aangegeven dat de met verwijdering belaste opsporingsambtenaar in dat geval het transport van de door het technisch hulpmiddel geregistreerde gegevens naar de technische infrastructuur beëindigt.[76]

De politie heeft in 2021 dit type verwijdering toegepast in een zaak waar het geautomatiseerd werk niet langer in gebruik leek bij de verdachte. Hiervan is een proces-verbaal door de politie opgemaakt.

Communicatie met leverancier technisch hulpmiddel

Tijdens de parlementaire behandeling van het wetsvoorstel CCIII is door de minister in beantwoording op vragen aangegeven dat in het kader van het onderzoek met een technisch hulpmiddel er geen verbinding tot stand gebracht wordt met een server van de maker van het technisch hulpmiddel. Er wordt uitsluitend een verbinding tot stand gebracht tussen het binnengedrongen geautomatiseerde werk en de server van de politie.[77] In de beantwoording geeft de minister aan dat de leverancier geen mogelijkheid heeft om zelfstandig updates uit te voeren en zelf de controle over het geautomatiseerd werk over te nemen. Evenmin kunnen andere klanten van de leverancier toegang krijgen tot het geautomatiseerd werk.[78]

In 2021 zijn in 15 zaken onderzoekshandelingen verricht met een technisch hulpmiddel dat een 'black box' is voor de politie. De leverancier van het technisch hulpmiddel heeft de servers die de politie hiervoor gebruikt in technisch beheer en kan hier op afstand op inloggen om beheer- en supportwerkzaamheden uit te voeren. Werkzaamheden die de leverancier uitvoert, kunnen, mogelijk zelfs tijdens uitvoering van een bevel, gevolgen hebben voor de werking en functionaliteit van het technisch hulpmiddel. De Inspectie merkt hierbij op dat deze wijze van toegang door de leverancier gebruikelijk is in de markt voor deze commerciële software. De politie stelt dat er geen alternatief voorhanden is dat dezelfde functionaliteit biedt zonder deze nadelen. Contractueel is afgesproken dat de leverancier uitsluitend inlogt op de servers na toestemming van de

[74] Zesde lid Artikel 126nba, Sv.
[75] *Kamerstukken II* 2015/16, 34 372 nr. 3 memorie van toelichting, p.36; *Kamerstukken II* 2016/17, 34 372 nr. 6, p.76.
[76] Bogw, artikel 26 eerste lid; *Kamerstukken II* 2015/16, 34 372 nr. 3 memorie van toelichting, p.36. "*Wanneer de software aanwezig blijft in het geautomatiseerde werk waarin de bevoegdheid is toegepast, wordt vanuit de server van de politie het dataverkeer stopgezet zodat de politie geen gegevens meer kan ontvangen van het geautomatiseerde werk.*"; *Kamerstukken II* 2016/17, 34 372 nr.6 p.78. "*Hier zien de opsporingsambtenaren van het technisch team op toe*".
[77] *Kamerstukken II* 2016/17, 34 372, nr.6 p.45 en p.51.
[78] *Kamerstukken II* 2016/17, 34 372, nr.6 p.74.

politie. De Inspectie heeft voorbeelden gezien van gevraagde toestemming die door de politie is verleend. Door het 'black box' karakter van het technisch hulpmiddel kan de politie de toegang door de leverancier echter niet technisch controleren of beperken. Tevens kan hierdoor niet gegarandeerd worden dat bij het gebruik van het technisch hulpmiddel uitsluitend verbindingen tot stand gebracht worden tussen het geautomatiseerde werk en de servers van de politie. De Inspectie merkt daarnaast op dat de door de politie verzamelde gegevens geruime tijd zijn opgeslagen in het technisch hulpmiddel waar ook de leverancier op afstand toegang toe heeft. Dit heeft de Inspectie ook in 2019 en 2020 geconstateerd. In reactie hierop heeft de minister benadrukt dat alleen het technisch team van de politie toegang heeft tot de servers waarop onderzoeksgegevens worden vastgelegd.[79] De Inspectie stelt vast dat de leverancier wel toegang heeft tot deze gegevens die in het technisch hulpmiddel zijn opgeslagen.

Centrale registratie toegang en toegangsverlening technisch hulpmiddel

In het Besluit is aangegeven dat voor toegang tot technische hulpmiddelen een formeel proces gevolgd moet worden dat vergelijkbaar is met het proces voor de registratie, uitgifte en inname van 'klassieke' technische hulpmiddelen (zoals een microfoon en/of een videocamera).[80] De korpschef wijst een of meer ambtenaren aan die belast zijn met de centrale registratie van de toegang tot technische hulpmiddelen. Deze ambtenaar verschaft toegang tot het technisch hulpmiddel aan de met plaatsing van het technisch hulpmiddel belaste opsporingsambtenaar voor de duur van het bevel. De ambtenaar die belast is met de centrale registratie registreert de naam van de opsporingsambtenaar die om toegang heeft verzocht, het tijdstip van toegangsverlening en enkele kenmerken van het technisch hulpmiddel.[81]

Evenals in 2020 stelt de Inspectie vast dat in 2021 binnen DIGIT geen proces geïmplementeerd was voor de registratie van toegang, uitgifte en inname van technische hulpmiddelen. In een reactie geeft de politie aan dat in overleg met de DIGIT officier van justitie afgeweken wordt van de eis voor centrale registratie en toegangsverlening tot technische hulpmiddelen omdat dit praktisch niet werkbaar zou zijn. De Inspectie merkt op dat begin 2022 DIGIT een systeem heeft geïmplementeerd waarmee de uitgifte van digitale sleutels (fysieke tokens) kan worden geregeld en geregistreerd. Hiermee kan deels tegemoet gekomen worden aan de in het Besluit voorgeschreven vereiste centrale registratie en toegangsverlening.

Onderzoekshandelingen middels handmatige inzet

Indien de officier van justitie besluit dat het verrichten van onderzoekshandelingen plaatsvindt zonder technisch hulpmiddel, dan worden procedurele waarborgen getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen. Het kunnen afleggen van verantwoording over de implementatie en opvolging van de aan DIGIT gestelde waarborgen op een

[79] *Kamerstukken II* 2020/21, 29 628, nr. 1030 p.7.
[80] Staatsblad 2006, nr. 524. 'Besluit technische hulpmiddelen strafvordering, dit Besluit is op 7 november 2006 in het Staatsblad gepubliceerd.
[81] Art. 22 Bogw en artikelsgewijze toelichting op artikel 22, p.45.

controleerbare en aantoonbare wijze is een belangrijk aspect voor de kwaliteit van de taakuitvoering door de politie.

In 2021 is in vijf zaken door de officier van justitie bevel gegeven voor het verrichten van onderzoekshandelingen zonder een technisch hulpmiddel. De Inspectie is aan de hand van het plan van aanpak en het journaal in deze zaken nagegaan welke waarborgen daartoe voor DIGIT voorzien waren en in welke mate deze waarborgen aantoonbaar getroffen en nageleefd zijn.

In vier van de vijf zaken vormt het maken van beeldschermopnamen en het vastleggen van toetsaanslagen van de onderzoekshandelingen onderdeel van de te treffen waarborgen. In één zaak kan de Inspectie op basis van het plan van aanpak, het journaal en de aanwezige processen-verbaal niet herleiden welke waarborgen door DIGIT getroffen moeten worden.

De Inspectie stelt vast dat DIGIT in 2021 niet in alle handmatige zaken de voorziene procedurele waarborgen getroffen heeft. In enkele zaken zijn de beeldschermopnames en registratie van toetsaanslagen niet volledig. Zie tevens hoofdstuk A.5.

Functiescheiding tussen technisch team en tactisch team

De resultaten van de onderzoekshandelingen worden ter beschikking gesteld aan de opsporingsambtenaren die zijn betrokken bij het operationele onderzoek, ook wel aangeduid als het tactisch team.[82] Om het risico van tunnelvisie te beperken moet volgens het Besluit gedurende het opsporingsonderzoek een strikte taakverdeling en functiescheiding tussen het technisch en het tactisch team aanwezig zijn.[83] De samenwerking moet dusdanig plaatsvinden dat het tactisch team geen enkele invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel of eigenstandig de werking van de software te beïnvloeden.[84] Tevens hebben de tactisch opsporingsambtenaren geen toegang tot de technisch infrastructuur waar de tijdens onderzoekhandelingen verkregen gegevens door het technisch team zijn vastgelegd.[85]

Volgens het journaal van het technisch team is in 2021 enkele malen contact geweest met leden van tactische teams over de inzet van een technisch hulpmiddel. De Inspectie heeft op basis van het journaal en de logging geen aanwijzingen dat tijdens deze contacten door DIGIT buiten de reikwijdte en perioden van het afgegeven bevel gehandeld is. De Inspectie toont begrip dat tijdens een operationele inzet hiertoe tussen de teams contacten zijn en dat de beoogde strikte scheiding in de praktijk niet altijd werkbaar is. De Inspectie heeft geen aanwijzingen dat leden van een tactisch team toegang hebben tot technische hulpmiddelen en de technische infrastructuur.

[82] Bogw, nota van toelichting p.14; *Kamerstukken II* 2015/16, 34 372 nr.3 p.14.
[83] *Kamerstukken II* 2016/17, 34 372 nr.6, p.28. Vanwege de functiescheiding wordt het onderzoek in een geautomatiseerd werk uitgevoerd door speciaal daarvoor opgeleide opsporingsambtenaren die niet betrokken zijn bij het betreffende opsporingsonderzoek.
[84] Bogw, nota van toelichting, p. 36; *Kamerstukken II* 2016/17, 34 372, nr. 6 p.40 en p.59; Bogw, nota van toelichting, p.17. "*De organisatorische scheiding tussen het technische team en het tactische team behoeft de samenwerking tussen de teams gedurende het opsporingsonderzoek niet te belemmeren. De officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt, vervult hierbij een schakelfunctie.*"
[85] Bogw, nota van toelichting, p.20; *Kamerstukken II* 2016/17, 34 372, nr.6, p.52.

A.5 Logging en andere verslaglegging

Onder logging verstaat het Besluit de elektronische verslaglegging over de uitvoering van een bevel.[86] Hierbij wordt onderscheid gemaakt tussen gegevens over:

- de verrichte handelingen tijdens de voorbereidende fase, het binnendringen in het geautomatiseerd werk alsmede de handelingen die gedurende de onderzoeksfase worden verricht.[87] De toelichting noemt dit 'inzetlogging'. Hierbij wordt de vastlegging genoemd van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar, de communicatie tussen de technische infrastructuur en het geautomatiseerd werk en gebruikte scripts en softwareversies.
- gegevens over de toegang tot een technisch hulpmiddel en het functioneren van de technische infrastructuur.[88] De toelichting noemt dit 'systeemlogging' die automatisch door alle gebruikte systemen wordt gegenereerd en centraal wordt verzameld en vastgelegd en betrekt hierbij ook de logging van toegang tot een technisch hulpmiddel;[89]
- gegevens over de ter uitvoering van het bevel door middel van onderzoekshandelingen verkregen gegevens (metadata);[90]

Een voorwaarde om te kunnen komen tot een juiste en volledige implementatie en controleerbare naleving van de logging is dat de politie zelf vastlegt en verantwoordt op welke wijze zij beoogt invulling te geven aan de vastlegging van gegevens over de uitvoering in logbestanden. De invulling en inrichting hiervan kan bovendien per zaak verschillen.

De Inspectie stelt vast dat de politie in 2021 een aanvang gemaakt heeft met het vastleggen en uitwerken van de wijze waarop zij invulling wil geven aan de diverse typen van logging die zijn beschreven in de nota van toelichting bij het Besluit. Deze uitwerking is in 2021 nog niet afgerond. Zo wordt in de uitwerking bijvoorbeeld nog geen aandacht besteed aan de situatie waarin gebruik gemaakt wordt van een ingekocht technisch hulpmiddel (waarvoor in 2021 in 23 zaken bevel is gegeven) of waarin opsporingshandelingen worden verricht vanaf een externe locatie. De implementatie van logging kan bovendien door het gebruik van verschillende middelen, de aard van de zaak en verschil in aanpak in concrete zaken afwijken.

Onderbelicht is tevens de toepassing en inrichting van systeemlogging. Volgens de toelichting bij het besluit wordt systeemlogging gebruikt voor het loggen van toegang tot een technisch hulpmiddel en voor het signaleren, onderzoeken en verhelpen van problemen met betrekking tot de betrouwbaarheid, integriteit en beschikbaarheid van de technische infrastructuur waarop de tijdens een onderzoek vergaarde gegevens worden vastgelegd.[91] De politie beperkt zich tot het benoemen dat over de gehele keten op alle gebruikte systemen systeemlogging plaatsvindt, zonder dit nader uit te werken. De Inspectie constateert dat de politie hiervoor als uitgangspunt heeft genomen wat technisch voorhanden is binnen de gekozen oplossing, in plaats van wat op basis van

[86] Bogw, nota van toelichting I, hoofdstuk 3.4 p.17.
[87] Art. 5 eerste lid sub a Bogw en artikelsgewijze toelichting artikel 5, p.36 waarin aangegeven is dat alle handelingen die tijdens het onderzoek in een geautomatiseerd werk plaatsvinden, worden gelogd.
[88] Art. 5 eerste lid sub b en d Bogw.
[89] Bogw, nota van toelichting, hoofdstuk 3.4 p.18.
[90] Art. 5 eerste lid sub d Bogw.
[91] Bogw, nota van toelichting, hoofdstuk 3.4, p.18

een risicoanalyse nodig is en volgt als vereiste uit het Besluit. Hierdoor wordt volgens de Inspectie nog niet aan al deze vereisten in de volle omvang invulling gegeven.

Daarnaast moet helder zijn wat deze technische infrastructuur omvat om invulling te kunnen geven aan het vastleggen van gegevens over het functioneren van de technische infrastructuur. De Inspectie heeft in 2020 geconstateerd dat de politie de reikwijdte van de technische infrastructuur nog niet bepaald had. De Inspectie stelt in 2021 vast dat de politie een aanzet gemaakt heeft voor het bepalen en vastleggen van de reikwijdte van de technische infrastructuur. Dit proces was in 2021 nog niet afgerond.

Het uitgangspunt voor deze logging is dat vastlegging doorlopend en automatisch plaatsvindt.[92] De gegevens over de verrichte handelingen (inzetlogging) mogen als uitzondering handmatig vastgelegd worden als deze gegevens naar hun aard niet automatisch vastgelegd kunnen worden.[93] De nota van toelichting benoemt in dit kader het journaal van de opsporingsambtenaar en de vastlegging van gebruikte scripts en softwareversies.[94]

De Inspectie stelt vast dat in 2021:
- op enkele kleine hiaten na, het samenstel van de automatisch en handmatig vastgelegde logging voldoende basis biedt voor het reconstrueren van alle in 2021 verrichte opsporingshandelingen op basis van de afgegeven bevelen;
- de volledigheid van de vastgelegde beeldschermopnames gedurende 2021 sterk is verbeterd. Zowel in 2019 als in 2020 en gedurende de eerste helft van 2021 was sprake van hiaten, mede doordat de voorziening voor het registreren van deze opnames niet goed functioneerde. Dit is inmiddels verbeterd;
- de politie is gestart met een volledigheidscontrole op de schermopnames van de handelingen die zijn verricht met het ingekochte technisch hulpmiddel voor de inzet waarvan in 23 van de 28 zaken bevel is gegeven. Zie tevens hoofdstuk A.8;
- in slechts één zaak de registratie van toetsaanslagen volledig is vastgelegd. Hierbij merkt de Inspectie op dat de registratie van toetsaanslagen in het merendeel van de zaken inhoudelijk geen waarde toevoegt;
- de politie is gestart met het testen van een softwarematige oplossing voor het vastleggen van beeldschermopnames en toetsaanslagen. Deze voorziening wordt ingezet bovenop de reeds aanwezige oplossing, waardoor het risico op ontbrekende beeldschermopnames en toetsaanslagen wordt verkleind;
- in de handmatige zaken niet vastgelegd is welke scripts ingezet zijn. Hierdoor is niet controleerbaar welke (versies van) scripts precies zijn ingezet en wat deze scripts deden;
- de journalisering sterk is verbeterd ten opzichte van de situatie in 2020. Verbeteringen zijn zichtbaar in de tijdigheid, detaillering en volledigheid. Wel heeft de Inspectie ook in 2021 in het journaal enkele verschrijvingen en omissies geïdentificeerd.

[92] Bogw, artikel 5, eerste lid en tweede lid.
[93] Bogw, artikel 5 tweede lid, handelingen naar hun aard niet automatisch vast te leggen; Bogw artikelsgewijze toelichting bij het Besluit, artikel 5, p.36; Bogw nota van toelichting hoofdstuk 3.4 p.17. *"De inzetlogging zal zoveel mogelijk geautomatiseerd plaatsvinden. Voor zover dit technisch niet mogelijk is, wordt procedureel binnen de politieorganisatie vastgelegd dat handmatige logging plaatsvindt."*
[94] Bogw, nota van toelichting hoofdstuk 3.4 p.17.

Belang logging en onregelmatigheid

De logging is in de eerste plaats van belang voor het uitvoeren van de interne controle door de politie op de verrichte handelingen en de controle op het functioneren van de technische infrastructuur.[95] Op basis van deze logging moet de politie zowel tijdens de uitvoering van een bevel als na afloop daarvan kunnen vaststellen of een onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de met de onderzoekshandelingen verkregen gegevens.[96] In aansluiting daarop moet de politie op basis van logging verantwoording kunnen afleggen in een strafzaak of als in het kader van het toezicht door de Inspectie JenV twijfels ontstaan over de verrichte handelingen en/of de betrouwbaarheid van het hiermee vergaarde bewijs.[97] Ook is de logging van belang mocht er sprake zijn van het optreden van schade en een mogelijke schadeclaim door betrokkene.[98]

De Inspectie stelt vast dat DIGIT in 2021 in een concept-document een definitie heeft opgenomen van het begrip onregelmatigheid. Een nadere uitwerking van welke gebeurtenissen de politie als 'onregelmatigheid' ziet, is in 2021 niet aangetroffen. Dit is van belang omdat de logging zodanig ingericht moet zijn dat aan de hand daarvan vastgesteld kan worden of deze onregelmatigheden hebben plaatsgevonden om daarover vervolgens te kunnen rapporteren.[99] De politie geeft in een reactie aan dat het uitputtend uitwerken van een onregelmatigheid niet direct voortvloeit uit een wettelijke verplichting. De politie kiest ervoor om dit te benaderen vanuit een eigen definitie van een onregelmatigheid en daar zelf aan te toetsen. De Inspectie stelt vast dat een controleerbaar afwegingskader ontbreekt, waardoor de eerste afweging of sprake is van een onregelmatigheid in belangrijke mate gebaseerd is op de professionele inschatting door individuele medewerkers van DIGIT. Daarnaast merkt de Inspectie op dat de door de politie geformuleerde definitie, een technische focus heeft op gebeurtenissen binnen de technische infrastructuur en niet op de gegevens zelf en ook niet op het gehele inzet-proces. Hierdoor worden procesmatige afwijkingen mogelijk niet als onregelmatigheid aangemerkt. Dit geldt tevens voor technische afwijkingen die optreden buiten de technische infrastructuur.

De politie kan hierdoor, zoals ook in 2020 door de Inspectie is geconstateerd, niet aantonen dat voldoende en juist gelogd wordt om het optreden van onregelmatigheden, zowel tijdens de uitvoering van het bevel als achteraf, te kunnen vaststellen.
Evenals in 2020 is niet door de politie uitgewerkt op welke wijze, door wie en wanneer het monitoren op onregelmatigheden vanuit een interne verantwoordelijkheid plaatsvindt. Dit heeft raakvlakken met de uitwerking van het kwaliteitssysteem in hoofdstuk A.8.

---

[95] Bogw, nota van toelichting, hoofdstuk 3.4, p.18. "*De logging is ten eerste en vooral bedoeld voor de interne controle van de tijdens de uitvoering van het bevel verrichte handelingen en het functioneren van de technische infrastructuur.*"; Bogw, Nota van Toelichting, hoofdstuk 3.4, p.18. In dat kader is tevens aangegeven dat voor het functioneren van de technische infrastructuur de systeemlogging gebruikt wordt voor het signaleren, onderzoeken en verhelpen van problemen met betrekking tot de betrouwbaarheid, integriteit en beschikbaarheid van de technische infrastructuur; *Kamerstukken I* 2016/17, 34 372 D, pagina 20. "*Op deze wijze kan zowel tijdens het verrichten van onderzoekshandelingen als achteraf intern toezicht plaatsvinden binnen de politieorganisatie op de uitvoering van het bevel van de officier van justitie*."

[96] Art. 6 eerste lid Bogw, vaststelling van onregelmatigheden; Bogw, nota van toelichting hoofdstuk 3.4 p.17,36.

[97] Bogw, nota van toelichting I, hoofdstuk 4, artikel 6 pagina 36. Vaststelling van onregelmatigheden.

[98] *Kamerstukken II* 2016/17 34 372, nr. 6, p.69 en p.80.

[99] Nota van toelichting Bogw, artikelsgewijze toelichting op art. 6, p. 36.

De Inspectie stelt vast dat in 2021:
- DIGIT aangeeft dat zij op basis van de loganalyses geen onregelmatigheden heeft gesignaleerd en gerapporteerd. Er door de afdeling security operations van DIGIT in 2021 geen onregelmatigheden zijn gemeld. Er in de processen-verbaal geen melding van onregelmatigheden door DIGIT is gedaan;
- hoewel enkele gebeurtenissen hebben plaatsgevonden die volgens de Inspectie mogelijk aangemerkt zouden kunnen worden als een onregelmatigheid, zijn er op basis van het journaal, de processen-verbaal en de beschikbare logging geen aanwijzingen dat er sprake is geweest van onregelmatigheden waarvan aannemelijk is dat ze invloed hebben gehad op de betrouwbaarheid en integriteit van de met de onderzoekshandelingen verkregen gegevens.

Betrouwbaarheid logbestanden

Gelet op het belang van de logging schrijft het Besluit voor dat de inhoud van logbestanden niet gewijzigd kan worden en dat de toegang tot logbestanden beperkt is tot alleen daartoe geautoriseerde personen.[100] Een uitwerking hiervan is dat de doorlopende en automatische logging over de uitgevoerde handelingen vastgelegd worden op een server van de politie[101] en dat leden van het technisch team geen toegang tot de logbestanden hebben.[102]

Zoals hiervoor is aangegeven constateert de Inspectie dat door de politie nog niet voor alle zaken is vastgelegd hoe en waar de doorlopende en automatische vastlegging van gegevens in logbestanden plaatsvindt. Deze uitwerking is van belang voor de politie om te kunnen komen tot het treffen van passende maatregelen voor de betrouwbaarheid en de integriteit van deze logbestanden.

De Inspectie stelt vast dat diverse logbestanden uiteindelijk worden vastgelegd in een voorziening die door de politie tot de technische infrastructuur gerekend wordt. Op basis van de netwerkarchitectuur en de getroffen maatregelen heeft de Inspectie geen aanwijzingen dat logbestanden die zijn ingebracht in deze technische voorziening kunnen worden aangepast. Uitsluitend beheerders van het infrastructuur beheerteam van DIGIT kunnen informatie hieruit verwijderen. Logbestanden kunnen uitsluitend in leesbare vorm uit deze technische infrastructuur worden gekopieerd door medewerkers die beschikken over de betreffende digitale sleutel (hardware token).

De Inspectie benadrukt dat maatregelen voor het waarborgen van de betrouwbaarheid van de logbestanden niet alleen binnen deze technische infrastructuur getroffen moeten worden, maar van belang zijn in het gehele loggingsproces. Hiermee doelt de Inspectie op het treffen van preventieve en repressieve maatregelen vanaf de bron waar deze logbestanden gegenereerd worden, tot en met het transport en de eventuele (tussentijdse) verwerking en opslag daarvan. Het loggingsproces zelf moet bovendien zo ingericht zijn dat de loggingsinformatie tijdens de fase van bewijsvergaring te allen tijde blijft functioneren en niet valt te manipuleren, te wijzigen of te verwijderen zonder dat dit achteraf zichtbaar is.[103] Een aandachtspunt is daarnaast dat maatregelen niet alleen gericht moeten zijn op de integriteit van de logbestanden, maar tevens op de

[100] Art. 7 Bogw en de artikelsgewijze toelichting op het Besluit artikel 7, p.37. Art. 7 tweede lid Bogw stelt dat logbestanden uitsluitend toegankelijk moeten zijn voor door de korpschef aangewezen ambtenaren.
[101] *Kamerstukken II* 2016/17, 34 372, nr.6, p. 52.
[102] *Kamerstukken II* 2016/17, 34372 nr. 6, p. 52 en p.59.
[103] *Kamerstukken II* 2016/17, 34 372, nr. 6, p.52 en p.59.

vertrouwelijkheid. Dit is vooral relevant voor de voorzieningen die verder af staan van de technische infrastructuur.

Vastgelegde gegevens (bewijslogging)

Door het technisch team verzamelde gegevens die kunnen dienen als bewijs in een strafzaak moeten vastgelegd worden op een technische infrastructuur.[104] Het Besluit definieert de technische infrastructuur als een technische voorziening van een technisch team bedoeld voor de vastlegging van gegevens ter uitvoering van een bevel.[105] De Inspectie heeft in 2020 geconstateerd dat de politie nog niet bepaald had wat de reikwijdte van de technische infrastructuur is, waardoor de Inspectie niet met zekerheid kon vaststellen of alle bewijslogging wel op de juiste plek en op betrouwbare wijze is vastgelegd. De Inspectie stelt in 2021 vast dat DIGIT een aanvang gemaakt heeft met het bepalen en vastleggen van de reikwijdte van de technische infrastructuur. Dit proces was in 2021 nog niet afgerond.

Volgens de toelichting op het Besluit dienen de betrouwbaarheid en integriteit van de vastgelegde gegevens onomstotelijk vast te staan, zowel in het belang van de betrokkene als in het belang van de opsporing.[106] De gegevens mogen niet inhoudelijk worden bewerkt en dienen te worden beveiligd tegen wijziging en kennisneming door onbevoegden. De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben daartoe geen toegang.[107] Vereist is dat de opslag van deze gegevens uitsluitend plaatsvindt op een beveiligde politieserver in beheer van de politie die zich in Nederland bevindt.[108] Voor de opslag van onderzoeksgegevens op de technische infrastructuur van de politie wordt geen gebruik gemaakt van een server van de leverancier van de (onderzoeks)software.[109]

Een belangrijk onderdeel van de door DIGIT bepaalde reikwijdte van de technische infrastructuur vormt een speciaal hiervoor ontwikkelde technische voorziening waar de bewijslogging uiteindelijk blijvend wordt opgeslagen. Ten aanzien van die voorziening en de gegevens die daarin opgeslagen zijn, stelt de Inspectie vast dat in 2021:

- de door DIGIT verkregen bewijslogging opgeslagen is in deze voorziening die onderdeel uitmaakt van de technische infrastructuur;
- maatregelen van kracht waren om de gegevens in deze voorziening te beschermen tegen wijzigingen en tegen kennisneming door onbevoegden;
- de gegevens uitsluitend toegankelijk waren voor medewerkers van DIGIT en de Inspectie;
- de opslag van de gegevens in deze voorziening plaatsvindt op een beveiligde politieserver in beheer van de politie die zich in Nederland bevindt.

De Inspectie stelt echter vast dat een gedeelte van de bewijslogging daarnaast ook is opgeslagen op locaties die door DIGIT niet tot de technische infrastructuur gerekend worden. In die situaties bevonden deze gegevens zich daar geruime tijd voordat sprake

[104] Art. 27 eerste lid Bogw. Vastlegging van gegevens op een technische infrastructuur.
[105] Artikel 1 lid g Bogw, definitie van een technische infrastructuur.
[106] Nota van toelichting Bogw hoofdstuk 3.7, p.21.
[107] Bogw, artikelsgewijze toelichting bij het Besluit, artikelen 27 en 28, p.47.
[108] Bogw, nota van toelichting, hoofdstuk 3.5 p. 18; Bogw, nota van toelichting, artikelsgewijze toelichting artikel 27 en 28; *Kamerstukken II* 2016/17, 34 372, nr.6, p.74.; *Kamerstukken II* 2018/19, 34. 372, nr. 29 p. 11 en p. 12.
[109] *Kamerstukken II* 2018/19, 34 372, nr. 29, p.12.

was van vastlegging binnen de technische infrastructuur. Deze tijdelijke opslag van een deel van de bewijslogging vond plaats op servers die technisch worden beheerd door een externe leverancier. Behoudens procedurele afspraken in een addendum bij het contract kan de politie niet waarborgen dat deze gegevens zijn beschermd tegen wijziging en onbevoegde kennisname door de leverancier.

Andere verslaglegging (proces-verbaal en journaal)

Een proces-verbaal is een officieel op papier gesteld verslag van de politie.[110] Een proces-verbaal vormt samen met het journaal en de elektronische logging een belangrijke waarborg voor de controleerbaarheid van de uitvoering van het bevel.[111] De verbaliseringsplicht houdt in dat de opsporingsambtenaren proces-verbaal[112] opmaken van de door hen verrichte handelingen zodat daarover verantwoording afgelegd kan worden.[113] In het journaal wordt door de opsporingsambtenaren, als een soort dagboek, handmatig verslaglegging gedaan over het procesverloop, de afspraken en de verrichtingen die zich niet lenen voor automatische vastlegging. Het journaal is een intern werkdocument van de politie dat niet bij de processtukken hoeft te worden gevoegd.[114]

De Inspectie stel vast dat in 2021:

- processen-verbaal kort na het afronden van de betreffende handelingen of het optreden van de betreffende gebeurtenissen zijn opgesteld en ondertekend. Dit is een verbetering ten opzichte van de situatie in 2019 en 2020;
- afgelegde verantwoording in enkele processen-verbaal op onderdelen niet geheel overeenkomt met de daadwerkelijke uitvoering. Zo is door de politie verklaard dat bepaalde maatregelen getroffen zijn of dat op een bepaalde wijze gehandeld is, terwijl de Inspectie vaststelt dat dit niet geheel juist is;
- DIGIT door de DIGIT officier van justitie geïnstrueerd is om in het belang van de afscherming van opsporingsmethodieken en -middelen minimaal te verbaliseren en maximaal te journaliseren. De Inspectie stelt vast dat de redenen van wetenschap in de processen-verbaal beperkt zijn vastgelegd. Een juist en volledig journaal wordt daarmee van nog groter belang;
- het journaal ten opzichte van 2020 volledi ger, gestructureerd en uniformer plaatsvindt en daarmee sterk verbeterd is. De gebruiksvriendelijkheid en toegankelijkheid van nieuw ontwikkelde tooling draagt daar in belangrijke mate aan bij;
- het journaal echter niet in alle gevallen juist is wanneer dit afgezet wordt tegen de feitelijke verrichtingen op basis van systeemlogging. Dit heeft gevolgen voor de juistheid van de processen-verbaal omdat de processen-verbaal gebaseerd zijn op de informatie uit het journaal.

Samenvattend constateert de Inspectie dat in het begin van 2021 de logging niet compleet was, net als in 2019 en 2020. In de loop van 2021 zijn deze problemen grotendeels verholpen door verbeteringen in de techniek. Het journaal was ook accurater en volledi ger. Door de logging en het journaal te combineren, heeft de

[110] https://www.politie.nl/informatie/wat-is-een-proces-verbaal.html
[111] *Kamerstukken II* 2015/16, 34372 nr. 3, p. 78.
[112] Zie wetboek van stafvordering art.152 (ten spoedigste), art. 153 (ambtseed, persoonlijk, gedagtekend, ondertekend en redenen van wetenschap), art. 156 (onverwijld toekomen).
[113] *Kamerstukken II* 2016/17 34 372, nr.6 p. 84.
[114] Aanwijzing opsporingsbevoegdheden. https://wetten.overheid.nl/BWBR0035498/2014-09-01

Inspectie de uitgevoerde handelingen in voldoende mate kunnen reconstrueren om een goed beeld te krijgen van de manier waarop de politie de hackbevoegdheid heeft toegepast. De Inspectie constateert echter ook dat de politie nog onvoldoende uitgewerkt en vastgesteld heeft wat de reikwijdte van de technische infrastructuur is en wat onregelmatigheden zijn. Door de politie is nog niet uitgewerkt en vastgesteld hoe en waar per zaak de doorlopende en automatische vastlegging in logbestanden plaatsvindt. De politie kan hierdoor niet aantonen dat passende maatregelen getroffen zijn om wijzigingen van de logbestanden of kennisneming hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of deze kennisneming heeft plaatsgevonden. Tevens kan door de politie niet worden aangetoond dat voldoende en juist gelogd wordt om zowel tijdens als na afloop van de uitvoering van een bevel onregelmatigheden te kunnen constateren.

A.6 Bewerking en verstrekking van vastgelegde gegevens

De resultaten van het onderzoek worden door het technisch team ter beschikking gesteld aan het tactisch team belast met het opsporingsonderzoek. Uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier van justitie vallen, mogen ter beschikking worden gesteld aan het tactisch onderzoeksteam.[115] Het kan hierbij nodig zijn om gegevens te filteren zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen, uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactisch team. Het technisch team draagt in dat geval zorg voor de selectie van onderzoeksgegevens.[116] Het Besluit stelt dat bij het maken van een selectie van vastgelegde gegevens sprake is van een bewerking. Op grond van het Besluit moet deze bewerking plaatsvinden op basis van een forensische kopie van de vastgelegde gegevens op een technische infrastructuur. In het proces-verbaal legt de opsporingsambtenaar de bewerkingen vast die plaatsgevonden hebben op deze kopie. Deze regels zijn van belang omdat de gegevens die tijdens de onderzoeksfase worden vastgelegd, kunnen worden gebruikt als bewijs in een strafzaak. Gelet hierop dienen de betrouwbaarheid en integriteit van de gegevens onomstotelijk vast te staan, zowel in het belang van de betrokkene als in het belang van de opsporing.[117]

De Inspectie stelt vast dat in 2021:
- het voor de Inspectie niet is vast te stellen welke gegevens precies zijn overgedragen aan de tactische teams omdat hier niet altijd logging en verslaglegging van is;
- DIGIT enkele malen een selectie heeft gemaakt van onderzoeksgegevens voor overdracht aan het tactisch team. Een deel van deze selecties is gemaakt op basis van een forensische kopie uit de technische infrastructuur, zodat de integriteit van de brongegevens maximaal is gewaarborgd. Enkele malen is bij het maken van tussentijdse selecties echter geen gebruik gemaakt van een forensische kopie uit de technische infrastructuur.

[115] *Kamerstukken II* 2016/17, 34 372, nr.6, p.14 en p.27.
[116] Bogw, nota van toelichting hoofdstuk 3.3, p. 17.
[117] Art. 29 Bogw en nota van toelichting hoofdstuk 3.7, p.21; Bogw, artikelsgewijze toelichting, artikel 29, p.48.

A.7 Bewaartermijnen, verwijdering en vernietiging gegevens

In de toelichting bij het Besluit is beschreven dat op grond van andere wettelijke bepalingen eisen gelden voor bewaartermijnen, verwijdering en vernietiging van verzamelde gegevens.[118]

Vanuit de kwaliteit van de taakuitvoering vloeit voort dat de politie haar processen, procedures en technische voorzieningen zodanig inricht en toepast dat op het moment dat de officier van justitie daartoe verzoekt, gegevens tijdig, juist en volledig worden vernietigd en verwijderd. Ook geldt hierbij dat deze gegevens juist en volledig bewaard en toegankelijk zijn en blijven gedurende de periode dat dat vereist wordt.

De Inspectie stelt vast dat in 2021:
- DIGIT op bevel van de officier van justitie gegevens heeft vernietigd die in 2020 waren verkregen van een geautomatiseerd werk met een kenmerk dat niet in het bevel was vermeld. DIGIT heeft van deze vernietiging processen-verbaal opgesteld;
- DIGIT deze gelegenheid heeft gebruikt om een werkinstructie op te stellen voor het verwijderen van bestanden in de technische infrastructuur. De instructie geeft naar oordeel van de Inspectie voldoende houvast voor een controleerbare, volledige en juiste verwijdering van bewijslogging gegevens die vastgelegd zijn in de technische infrastructuur van DIGIT. De instructie beschrijft echter niet hoe alle te verwijderen bestanden geïdentificeerd moeten worden. Na uitvoering van de vernietiging bleek nog een back-up aanwezig te zijn met de betreffende gegevens. Deze back-up is, nadat de Inspectie de politie hierop heeft gewezen, alsnog verwijderd. Hiervan is in 2021 nog geen proces-verbaal opgesteld;
- DIGIT bevel heeft gekregen gegevens te vernietigen omdat een zaak uit 2019 is geëindigd en de betrokkene schriftelijk door de officier van justitie in kennis is gesteld[119] van het feit dat heimelijk is binnengedrongen in een geautomatiseerd werk en onderzoekshandelingen zijn verricht. De politie heeft aan dit vernietigingsbevel uitvoering gegeven en hiervan in 2021 voor een deel van de uitgevoerde vernietiging processen-verbaal opgesteld. Voor het resterende deel van de vernietiging bevonden de processen-verbaal zich volgens DIGIT begin 2022 nog in het proces van vaststelling. De Inspectie heeft hierbij geen afwijkingen geconstateerd van de wettelijke bepalingen en zal de nog op te stellen processen-verbaal betrekken in haar toezicht over 2022.

De Inspectie constateert dat vanuit andere wetgeving onderscheid gemaakt wordt tussen vernietiging en verwijdering van gegevens. De Inspectie merkt op dat DIGIT nog geen werkinstructie heeft opgesteld voor verwijdering van politiegegevens die niet langer nodig zijn voor het doel van het onderzoek.[120] Deze verwijderde politiegegevens dienen gedurende een termijn van vijf jaar bewaard te worden ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen.[121] Deze situatie heeft zich gelet op de nog relatief korte periode waarin de bevoegdheid door de politie ingezet mag worden, in 2021 niet voorgedaan, maar vraagt wel aandacht zodat hierop door de politie tijdig geanticipeerd wordt.

[118] Bogw, nota van toelichting, hoofdstuk 4, p 22, (Gegevensverwerking).
[119] Via een notificatie zoals beschreven in artikel 126bb Sv
[120] Zoals voorgeschreven in art. 9 lid 4 Wpg
[121] Art. 14 eerste lid Wpg

A.8 Informatiebeveiliging, kwaliteitssysteem en interne controle

De betrouwbaarheid, integriteit en herleidbaarheid van gegevens is cruciaal voor het gebruik van de verkregen gegevens als bewijs in een strafzaak. Volgens het Besluit dienen hiertoe maatregelen getroffen te worden om onbevoegde kennisname en het wijzigen van deze gegevens te voorkomen en om achteraf te kunnen vaststellen of hiervan sprake was. Op de politie zijn wettelijke regelingen[122] van toepassing die aanknopingspunten bieden voor een nadere invulling van deze maatregelen. De politie dient op basis hiervan te komen tot een samenhangend geheel van te treffen beheersingsmaatregelen, die zijn afgestemd op de risico's.

De beheersing van beveiligingsrisico's is van belang om te waarborgen dat passende beheersingsmaatregelen voor de betrouwbaarheid en integriteit van de logging en de technische infrastructuur getroffen worden en zijn. Dit vormt de basis om door de politie vanuit een interne verantwoordelijkheid toe te zien op het inrichten van deze maatregelen, de structurele naleving daarvan en daarover op een controleerbare wijze verantwoording af te kunnen leggen. De Inspectie ziet hierop toe vanuit haar toezicht op de kwaliteit van de taakuitvoering door de politie.[123]

De Inspectie heeft in haar verslag over 2020 gerapporteerd dat DIGIT de eerste stappen had gezet om te komen tot een aantoonbaar en controleerbaar passend beveiligingsniveau. In 2021 constateert de Inspectie dat er geen vooruitgang geboekt is in de benodigde doorontwikkeling en vervolgstappen.

In een reactie geeft DIGIT aan dat het vertalen en operationaliseren van beheersingsmaatregelen in de praktijksituatie weerbarstig is gebleken. In een breder politie-verband vindt volgens DIGIT een herbezinning plaats over de kaders en maatregelen die voor dergelijke omgevingen toegepast moeten worden. De Inspectie heeft in 2021 geen inhoudelijke kennis kunnen nemen van uitgewerkte plannen. De Inspectie zal deze ontwikkeling en de voortgang gedurende 2022 blijven monitoren.

Dit betekent dat, evenals in 2020, ook in 2021 DIGIT onvoldoende is nagegaan of haar processen en systemen voldoen aan de door de politie gestelde beveiligingseisen. De politie heeft evenals in 2020 nog geen compleet en samenhangend pakket van door DIGIT te treffen beveiligingsmaatregelen vastgesteld. De Inspectie stelt vast dat DIGIT in 2021 geen aantoonbare verantwoording kon overleggen over de inrichting van beveiligingsmaatregelen en het functioneren daarvan. De Inspectie kan hierdoor in 2021 voor haar toezicht niet steunen op een intern beheersingsmechanisme ten aanzien van informatiebeveiliging.

Om eventuele risico's in perspectief te kunnen plaatsen, heeft de Inspectie ook zelf gekeken naar de implementatie van maatregelen waaronder de inrichting van logische toegangsbeveiliging. Op specifieke onderdelen zijn er door DIGIT in 2021 technische verbeteringen doorgevoerd. Hoewel de Inspectie enkele tekortkomingen heeft

[122] Regeling Informatiebeveiliging Politie (RIP, https://wetten.overheid.nl/BWBR0008599/2017-12-15 en Wet politiegegevens (Wpg, https://wetten.overheid.nl/BWBR0022463/2020-01-01). Tevens heeft de politie zich gecommitteerd aan de Baseline Informatiebeveiliging Overheid (BIO) en zijn in een addendum per rubriceringsniveau door de politie specifiek te treffen maatregelen vastgesteld (BIO+).

[123] Art. 65 Politiewet 2012.

gesignaleerd in het autorisatiebeheer, heeft zij op basis van haar waarnemingen geen aanwijzingen voor grote technische beveiligingsrisico's in de technische infrastructuur van DIGIT.

Kwaliteitssysteem en interne controle

In de nota van toelichting bij het Besluit is aangegeven dat de Inspectie systeemtoezicht uitoefent, hetgeen een vorm van interne controle of interne borging binnen de politie veronderstelt. Het belang van de interne controle wordt ook onderstreept in de toelichting bij het Besluit waarbij aangeven is dat de logging ten eerste en vooral bedoeld is voor de interne controle van de tijdens de uitvoering van het bevel verrichte handelingen en het functioneren van de technische infrastructuur.[124]

De Inspectie houdt toezicht op de kwaliteit van de taakuitvoering door de politie.[125] Een intern kwaliteitssysteem waaronder een eigen interne controle is een belangrijk onderdeel voor het borgen van deze kwaliteit. Met een dergelijk systeem kan de politie zelf de kwaliteit van de inzet van de bevoegdheid tijdens alle fasen van de uitvoering borgen en eventuele onregelmatigheden en tekortkomingen hierin tijdig identificeren en verhelpen.[126] Hierbij kan bijvoorbeeld gedacht worden aan controles ten aanzien van de kwaliteit van het journaal, haalbaarheidsonderzoeken, processen-verbaal, volledigheid van logging en het adequaat functioneren van voorzieningen voor het doorlopend en automatisch vastleggen van handelingen. Dit is van belang voor een rechtmatige toepassing van de bevoegdheid door de politie.

In haar verslag over 2020 constateerde de Inspectie dat de politie niet beschikte over een goed functionerend kwaliteitssysteem (inclusief interne controle) om de kwaliteit van de inzet van deze bevoegdheid tijdens alle fasen van de uitvoering te borgen en eventuele onregelmatigheden en tekortkomingen hierin tijdig te identificeren en te verhelpen. Ook werd door de Inspectie in haar verslag over 2020 vermeld dat de politie soms fouten en hiaten in de verslaglegging niet zelf opmerkte en dat zij onvoldoende toeziet op de kwaliteit van documenten. In de loop van 2021 heeft de Inspectie een aantal verbeteringen geconstateerd en de positieve effecten daarvan op de kwaliteit in de dagelijkse praktijk gezien. Op onderdelen is door DIGIT in 2021 een vorm van kwaliteitsbewaking en interne controle verder ingericht. Voorbeelden zijn de realisatie van een dashboard voor het controleren of schermopnames en registraties van toetsaanslagen actief zijn, de controles die worden uitgevoerd door de dossiervormers en de volledigheidscontroles op de schermopnames van de inzet van het ingekochte technische hulpmiddel. Daarnaast is nieuwe functionaliteit toegevoegd voor het automatisch inrichten van beperkingen en controles in een systeem dat DIGIT veel gebruikt voor het binnendringen en het doen van onderzoek. Deze functionaliteit heeft ervoor gezorgd dat onregelmatigheden zijn voorkomen.

De Inspectie merkt opdat de politie nog niet in beeld heeft gebracht voor welke onderdelen van de belangrijkste (werk)processen kwaliteitsbewaking en interne controle moet worden ingericht. Een overkoepelende visie waarin deze activiteiten in samenhang gebracht zijn en welke instrumenten daartoe door wie, wanneer moeten worden ingezet, is nog niet gereed. Niet bepaald is wie precies welke taken en verantwoordelijkheden

[124] Bogw, nota van toelichting, p.18.
[125] Art. 65 Politiewet 2012.
[126] *Kamerstukken II* 2016/17, 34 372, nr.6, p.59.

hierin heeft. Ook is niet bepaald hoe en aan wie verantwoording wordt afgelegd. Tevens ontbreekt documentatie om de kwaliteit van de taakuitvoering te borgen en te voorkomen dat dit uitsluitend rust op de professionele inschatting van individuele medewerkers. Hierdoor ontbreekt structurele borging. DIGIT was in 2021 nog bezig met het uitwerken en vastleggen van het beoogde kwaliteitssysteem waaronder de interne controles. De Inspectie heeft daarvan in 2021 nog geen kennis kunnen nemen.

Bijlage B: Afkortingen

Afkorting	**Betekenis**
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AP	Autoriteit Persoonsgegevens
Bogw	Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in artt. 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), Stb. 2018, 340.
CCIII	Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III)
DIGIT	Digital Intrusion Team (onderdeel van de Landelijke Eenheid van de Nationale Politie). Het technisch team dat is belast met de uitoefening van de hackbevoegdheid maakt deel uit van DIGIT.
OM	Het Openbaar Ministerie
PG-HR	Procureur-generaal bij de Hoge Raad der Nederlanden
TNO	De Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek

Inspectie Justitie en Veiligheid

Toezicht, omdat rechtvaardigheid en veiligheid niet vanzelfsprekend zijn.

Dit is een uitgave van:
Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP Den Haag
Postbus 20301 | 2500 EH Den Haag
Contactformulier | www.inspectie-jenv.nl

April 2022

Aan deze publicatie kunnen geen rechten worden ontleend. Vermenigvuldigen van informatie uit deze publicatie is toegestaan, mits deze uitgave als bron wordt vermeld.